INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 14:08 UTC

AD CS Exploitation Persists: ESC1, Shadow Credentials, and Detection Gaps Enable Domain Compromise

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0124
Type	Security Analysis
CVE ID	CVE-2022-26923
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Active Directory Certificate Services (AD CS), Windows Hello for Business, Kerberos/PKINIT authentication
Published	2026-05-11T22:00:43+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Active Directory Certificate Services (AD CS) remains an actively exploited escalation path enabling full domain compromise from low-privileged footholds, with ransomware operators and state-sponsored actors both documented as active exploiters. Unit 42's analysis confirms a five-phase attack lifecycle that bypasses signature-based defenses, anchored by CVE-2022-26923 (CVSS 7.5) and misconfigured certificate templates that most organizations leave in place out of fear of disrupting legacy authentication workflows. The persistence of this threat reflects a structural gap: known-exploitable configurations are present in production because template modification introduces operational change risk that many organizations defer, creating a window where the security risk remains unmitigated.

Technical Analysis

AD CS exploitation has graduated from a niche post-exploitation technique to a reliable primary escalation path used by ransomware operators and nation-state actors alike. Unit 42's analysis documents the attack chain across five phases, each with distinct tooling and behavioral signatures that security teams can instrument for detection.

The attack typically begins with a low-privileged foothold, compromised credentials, a phishing lure, or supply chain access, and then pivots to certificate abuse. The ESC1 misconfiguration is the most commonly

weaponized template flaw: when a certificate template allows requesters to supply an arbitrary Subject Alternative Name (SAN), an attacker can request a certificate asserting the identity of any user in the domain, including domain administrators. This certificate is then used through Kerberos PKINIT authentication (T1558, T1550.003) to obtain a Ticket Granting Ticket (TGT) as the impersonated account.

Shadow credentials (a variant of T1649, Steal or Forge Authentication Certificates) extend this surface. By writing to the msDS-KeyCredentialLink attribute of a target object, possible whenever an attacker holds write permissions on that object, attackers plant a certificate credential that survives password resets. This technique is particularly dangerous because it establishes persistence that conventional credential hygiene does not remediate.

CVE-2022-26923 (NVD, Microsoft MSRC) is the anchor vulnerability: a privilege escalation flaw in the AD CS enrollment process affecting Windows environments running Windows Hello for Business. An authenticated attacker can craft a certificate request that impersonates a domain controller, enabling full domain compromise. Microsoft patched this in May 2022, but patch deployment and template remediation are not synonymous, vulnerable template configurations persist in patched environments.

The institutional blind spot Unit 42 identifies is operationally significant: administrators frequently decline to modify legacy certificate templates because doing so risks breaking authentication workflows for services, devices, and users dependent on those templates. This produces a documented, exploitable condition that survives patch cycles.

The MITRE ATT&CK footprint is broad: T1134 (Access Token Manipulation), T1136 (Create Account), T1558 (Steal or Forge Kerberos Tickets), T1078 (Valid Accounts), T1550.001 (Application Access Token), T1484 (Domain Policy Modification), T1649 (Steal or Forge Authentication Certificates), T1552.001 (Credentials in Files), T1550.003 (Pass the Ticket), and T1195.002 (Compromise Software Supply Chain) are all mapped to this campaign pattern. The breadth of this mapping reflects how AD CS exploitation serves as both an initial access amplifier and a persistence mechanism, not merely a privilege escalation step.

Detection coverage noted for Palo Alto Cortex XDR and XSIAM specifically, with behavioral analytics targeting certificate enrollment anomalies and Kerberos ticket abuse patterns. Organizations without these platforms should review their SIEM and EDR coverage against the behavioral patterns documented in the five-phase lifecycle.

Action Checklist

1. Step 1: Assess exposure, determine whether your environment runs Active Directory Certificate Services with any certificate templates configured for client authentication. Audit specifically for ESC1 conditions: templates that allow Subject Alternative Name specification by the requester, combined with overly permissive enrollment permissions (authenticated users or domain computers).
2. Step 2: Review controls, verify patch status for CVE-2022-26923 across all domain controllers and CA servers (Microsoft patched May 2022). Separately audit certificate template configurations using tools such as Certify or PSPKIAudit to identify ESC1 through ESC8 misconfigurations. Confirm that msDS-KeyCredentialLink attribute write permissions are restricted to intended principals to limit shadow credential abuse.
3. Step 3: Update threat model, add AD CS certificate template abuse (ESC1), shadow credential persistence (T1649), and Kerberos PKINIT ticket forging (T1558/T1550.003) to your threat register. Flag both ransomware operator and state-sponsored actor categories as active exploiters of this path per

recent threat intelligence reporting.

4. Step 4: Communicate findings, brief leadership on whether your organization's AD CS deployment has been assessed for template misconfigurations. Frame the risk specifically: a low-privileged compromised account can become a domain administrator without triggering password-based detection, and this path is actively used in ransomware pre-deployment phases.

5. Step 5: Monitor developments, track published indicators and follow-up analysis. Monitor CISA advisories and Microsoft MSRC for CVE-2022-26923 status; if escalated to the Known Exploited Vulnerabilities catalog, remediation becomes mandated in federal and regulated environments.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to incident response if Event ID 4887 shows any certificate issued with a SAN value matching a privileged account (Domain Admin, Enterprise Admin, Schema Admin) from a non-privileged requester, or if any msDS-KeyCredentialLink value is detected on a privileged account that was not placed there by an authorized provisioning system — either condition indicates active exploitation of CVE-2022-26923 or shadow credential abuse and constitutes a domain-level compromise requiring breach notification assessment under applicable regulatory frameworks (HIPAA, PCI-DSS, SEC Cybersecurity Disclosure Rules).
Recovery Notes	After containing an AD CS compromise, revoke all certificates issued from ESC1-vulnerable templates during the exploitation window using `certutil -revoke ` and publish a new CRL immediately via `certutil -crl` on the CA server — do not rely on certificate expiration to neutralize forged credentials. Remediate template misconfigurations by disabling ENROLLEE_SUPPLIES_SUBJECT flag (msPKI-Certificate-Name-Flag) on vulnerable templates and restricting enrollment permissions to named service accounts rather than Authenticated Users or Domain Computers. Monitor Event ID 4769 (Kerberos TGS requests) filtered for PKINIT pre-authentication for a minimum of 30 days post-remediation to detect any attacker-held certificates still generating valid Kerberos tickets before the revocation chain propagates fully.

Forensic Artifacts	CA Server Windows Security Event Log — Event IDs 4886 (certificate request received), 4887 (certificate issued), and 4888 (request denied): filter for SAN field values containing privileged account UPNs (administrator@, DA accounts) submitted by non-privileged requesters, which is the direct forensic signature of ESC1 exploitation via CVE-2022-26923 | Active Directory attribute replication metadata for msDS-KeyCredentialLink on all privileged accounts: run `Get-ADReplicationAttributeMetadata` to identify unauthorized writes with timestamps, originating DC, and writing principal — shadow credential insertion by an attacker will appear as a write from a non-standard principal (not SYSTEM, Key Admins, or Azure AD Connect) | Domain Controller Kerberos Event Log — Event ID 4768 (TGT request) and 4769 (TGS request) filtered for certificate-based pre-authentication (PA-TYPE 17/16 in the pre-authentication data field): PKINIT-based ticket requests using forged or ESC1-obtained certificates will appear here and are distinct from password-based Kerberos flows | Registry key `HKLM\SYSTEM\CurrentControlSet\Services\Kdc\StrongCertificateBindingEnforcement` on all DCs: a value of 0 confirms the CVE-2022-26923 patch enforcement mode is disabled regardless of KB5014754 installation status, and this key state is forensically significant to establishing exploitability at the time of any suspected incident | Certutil CA database export (`certutil -view -out RequestID,RequesterName,SubjectAltName,NotBefore,NotAfter csv > ca_issued_certs.csv`): this flat-file export of all issued certificates allows offline timeline analysis to identify any certificate whose SAN differs from the requester's own identity, the definitive artifact of ESC1 exploitation without requiring SIEM access

Per-Action IR Details

Step 1: Assess exposure — determine whether your environment runs Active Directory Certificate Services with any certificate templates configured for client authentication. Audit specifically for ESC1 conditions: templates that allow Subject Alternative Name specification by the requester, combined with overly permissive enrollment permissions (authenticated users or domain computers).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and understanding asset exposure before an incident occurs

Controls: NIST SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), NIST CM-6 (Configuration Settings), NIST CA-7 (Continuous Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run Certify.exe (GhostPack) as a low-privileged domain user: `Certify.exe find /vulnerable` — this enumerates templates with msPKI-Certificate-Name-Flag set to ENROLLEE_SUPPLIES_SUBJECT and overly broad enrollment ACLs. Alternatively, use PSPKIAudit (free, PowerShell): `Invoke-PKIAudit` outputs ESC1–ESC8 findings without requiring admin rights. Cross-reference output against `certutil -catemplates` to confirm which templates are actively published on your CA.

Evidence: Before auditing, snapshot the current state of certificate templates for baseline comparison: export `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\\CAServerName` and run `certutil -v -dstemplate > templates_baseline.txt`. Capture the msDS-KeyCredentialLink attribute state for high-value accounts (domain admins, service accounts) via `Get-ADUser -Filter * -Properties msDS-KeyCredentialLink | Where-Object {$_.msDS-KeyCredentialLink -ne $null}`. This pre-audit snapshot establishes the forensic baseline needed to detect shadow credential insertion post-compromise.

Step 2: Review controls — verify patch status for CVE-2022-26923 across all domain controllers and CA servers (Microsoft patched May 2022). Separately audit certificate template configurations using tools such as Certify or PSPKIAudit to identify ESC1 through ESC8 misconfigurations. Confirm that msDS-KeyCredentialLink attribute write permissions are restricted to intended principals to limit shadow credential abuse.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring systems are hardened and controls are verified prior to exploitation

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify CVE-2022-26923 patch (KB5014754) deployment across all DCs with: `Get-HotFix -Id KB5014754 -ComputerName (Get-ADDomainController -Filter *).Name | Select PSComputerName,InstalledOn`. For msDS-KeyCredentialLink ACL review without enterprise tooling, run: `(Get-ACL 'AD:CN=,DC=domain,DC=com').Access | Where-Object {$_.ActiveDirectoryRights -match 'WriteProperty' -and $_.ObjectType -eq '5b47d60f-6090-40b2-9f37-2a4de88f3063'}` — that GUID is the msDS-KeyCredentialLink attribute schema ID. Flag any principal outside SYSTEM, Domain Admins, and Key Admins.

Evidence: Collect patch compliance evidence before proceeding: run `wmic qfe list full /format:csv > dc_patch_inventory.csv` on each DC and CA server. For CVE-2022-26923 specifically, confirm the StrongCertificateBindingEnforcement registry key value at `HKLM\SYSTEM\CurrentControlSet\Services\Kdc\StrongCertificateBindingEnforcement` — a value of 0 on any DC means the patch enforcement mode is disabled and the system remains exploitable despite patching. Capture Active Directory replication metadata for msDS-KeyCredentialLink on privileged accounts using `Get-ADReplicationAttributeMetadata -Object -Server -ShowAllLinkedValues` to identify any unauthorized writes that predate your audit.

Step 3: Update threat model — add AD CS certificate template abuse (ESC1), shadow credential persistence (T1649), and Kerberos PKINIT ticket forging (T1558/T1550.003) to your threat register. Flag both ransomware operator and state-sponsored actor categories as active exploiters of this path per Unit 42 May 2026 reporting.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: integrating threat intelligence to improve detection accuracy and prioritize monitoring

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Map Unit 42's five-phase AD CS attack lifecycle directly to MITRE ATT&CK: initial foothold → T1078 (Valid Accounts), ESC1 template abuse → T1649 (Steal or Forge Authentication Certificates), PKINIT ticket request → T1558 (Steal or Forge Kerberos Tickets), lateral movement → T1550.003 (Pass the Ticket), ransomware pre-deployment → T1486 (Data Encrypted for Impact). Add Sigma rules from SigmaHQ for certificate services abuse (search `sigma/rules/windows/builtin/security/` for `win_security_certificate_request` and `win_ad_account_enumeration`) to deploy against Windows Security event logs without a SIEM — parse with `sigma convert -t powershell` and schedule via Task Scheduler.

Evidence: Before updating the threat model, pull historical Windows Security Event Log Event ID 4886 (Certificate Services received a certificate request) and Event ID 4887 (Certificate Services approved a certificate request and issued a certificate) from the CA server going back 90 days — ESC1 exploitation will show certificate requests where the SAN field contains a privileged account UPN (e.g., administrator@domain.com) submitted by a non-privileged requester account. Also extract Event ID 4769 (Kerberos Service Ticket Request) filtered for ticket encryption type 0x11 or 0x12 (AES) with certificate-based pre-authentication (PA-DATA type 17 or 16), which indicates PKINIT usage that may represent forged ticket activity.

Step 4: Communicate findings — brief leadership on whether your organization's AD CS deployment has been assessed for template misconfigurations. Frame the risk specifically: a low-privileged compromised account can become a domain administrator without triggering password-based detection, and this path is actively used in ransomware pre-deployment phases.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: communicating incident scope and impact estimates to authorized staff and leadership

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST IR-4 (Incident Handling), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Produce a one-page AD CS risk brief quantified with output from Certify or PSPKIAudit: state the number of ESC1-vulnerable templates found, the number of principals with enrollment rights (from `Get-ADGroupMember 'Authenticated Users'` scope), and the blast radius — any of those principals can request a certificate impersonating Domain Admin without a password change. Reference the Unit 42 May 2026 finding that ransomware operators use this path specifically in the pre-deployment phase to establish persistence before encryption begins, making it a direct business-continuity risk.

Evidence: Gather supporting evidence for the leadership brief before the meeting: export the output of `Certify.exe find /vulnerable` with template names, enrollment permissions, and SAN flags clearly identified. Pull a 90-day count of certificate issuances from Event ID 4887 on the CA server, broken down by requesting account, to show leadership whether certificate issuance volume is anomalous. If any certificate was issued to a SAN value matching a privileged account (DA, EA, Schema Admin) from a standard user requester, document that finding explicitly — it may indicate active exploitation requiring immediate escalation beyond a briefing.

Step 5: Monitor developments — track Unit 42's published indicators and follow-up analysis at the source URL. Monitor CISA advisories and Microsoft MSRC for any escalation of CVE-2022-26923 to the Known Exploited Vulnerabilities catalog, which would trigger mandatory remediation timelines in federal and regulated environments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: updating policies, improving detection capability, and integrating threat intelligence to prevent recurrence

Controls: NIST IR-5 (Incident Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-8 (Incident Response Plan), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Subscribe to the CISA KEV RSS feed (https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json) and parse it with a daily cron job or scheduled PowerShell task that alerts if CVE-2022-26923 appears: `Invoke-RestMethod -Uri 'https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json' | Select-Object -ExpandProperty vulnerabilities | Where-Object {$_.cveID -eq 'CVE-2022-26923'}`. For continuous AD CS monitoring without a SIEM, deploy a scheduled task on the CA server that exports new Event ID 4887 issuances daily and emails the list to the security team for manual review of SAN field values.

Evidence: Maintain ongoing collection of CA server Event IDs 4886, 4887, and 4888 (certificate request denied) as your persistent forensic baseline for AD CS activity. Additionally, configure persistent monitoring of the msDS-KeyCredentialLink attribute by scheduling `Get-ADUser -Filter * -Properties msDS-KeyCredentialLink | Where-Object {$_.msDS-KeyCredentialLink -ne $null} | Export-Csv msds_keycredentiallink_snapshot_$(Get-Date -Format yyyyMMdd).csv` daily — delta comparison between daily snapshots will surface unauthorized shadow credential additions targeting privileged accounts, which is the persistence mechanism Unit 42 documented as surviving password resets and remaining undetected by password-based monitoring.

Detection Guidance

Detection for AD CS exploitation requires behavioral analytics beyond signature matching. Key areas to instrument:

Certificate Enrollment Anomalies: Monitor AD CS enrollment logs (Event ID 4886 and 4887 on the CA server) for certificate requests where the Subject Alternative Name differs from the requesting account's identity.

Flag any certificate issued to a non-CA account asserting a domain controller or privileged account identity. Note: The following detection strategies assume Windows CA role is deployed. Organizations without on-premise CA infrastructure should focus on endpoint-based Kerberos authentication anomalies.

msDS-KeyCredentialLink Writes: Alert on writes to the msDS-KeyCredentialLink attribute on user or computer objects (Windows Security Event ID 5136, Directory Service Object Modified). Legitimate writes are rare and typically originate from Windows Hello for Business provisioning. Any write from an unexpected principal warrants investigation.

Kerberos PKINIT Abuse: Hunt for Kerberos TGT requests using certificate-based pre-authentication (Event ID 4768 with pre-authentication type 16) issued to accounts that do not normally use certificate-based logon. Cross-correlate with recent certificate enrollment events for the same account.

Privilege Escalation Indicators: Monitor for rapid privilege transitions, accounts accessing high-value targets (domain controllers, backup infrastructure, secrets stores) shortly after certificate enrollment events. T1134 (token manipulation) and T1484 (domain policy modification) behavioral patterns should be baselined and alerted.

Tool Behavior: Certify.exe, Certipy, and PKINITtools are common attacker-side tools for this exploitation path. Monitor for execution of unsigned binaries querying AD CS enrollment endpoints, LDAP queries targeting certificate template objects, and anomalous use of the PKINIT protocol from workstation-class machines.

Log Sources: Windows CA audit logs, Active Directory audit logs (DS Access auditing enabled), Kerberos authentication events on domain controllers, and EDR process/network telemetry from endpoints performing certificate enrollment operations.

Detection coverage is documented for Cortex XDR and XSIAM; organizations on other platforms should map these behavioral indicators to available SIEM/SOAR detection logic.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Certify.exe`	Certify leveraged during AD CS reconnaissance phase to enumerate misconfigured certificate templates (ESC1) and identify exploitable enrollment permissions within the domain	HIGH
TOOL	`Certipy`	Certipy (Python-based) leveraged to request certificates exploiting ESC1 template misconfigurations and perform shadow credential attacks via msDS-KeyCredentialLink attribute writes	HIGH
TOOL	`PKINITtools`	PKINITtools leveraged post-certificate-issuance to perform Kerberos PKINIT authentication and obtain TGTs impersonating privileged domain accounts, enabling pass-the-ticket lateral movement	HIGH

Type	Value	Context	Confidence
URL	`Pending — refer to Unit 42 (https://unit42.paloaltonetworks.com/active-directory-certificate-services-exploitation/) for published indicators`	Unit 42 May 2026 analysis documents attacker tooling and behavioral patterns across a five-phase exploitation lifecycle; specific hashes, C2 infrastructure, or additional IOC values should be retrieved directly from the source report	LOW

Framework Mappings

MITRE-ATTACK

- **T1134** — Access Token Manipulation
- **T1136** — Create Account
- **T1558** — Steal or Forge Kerberos Tickets
- **T1078** — Valid Accounts
- **T1550.001** — Application Access Token
- **T1484** — Domain or Tenant Policy Modification
- **T1649** — Steal or Forge Authentication Certificates
- **T1552.001** — Credentials In Files
- **T1550.003** — Pass the Ticket
- **T1195.002** — Compromise Software Supply Chain

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection
- **SI-4** — System Monitoring

OWASP-TOP10-2021

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

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **3.3** — Configure Data Access Control Lists
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1134	Access Token Manipulation	Defense-Evasion
T1136	Create Account	Persistence
T1558	Steal or Forge Kerberos Tickets	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion
T1484	Domain or Tenant Policy Modification	Defense-Evasion
T1649	Steal or Forge Authentication Certificates	Credential-Access

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access
T1550.003	Pass the Ticket	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/active-directory-certificate-se...	T3
	https://unit42.paloaltonetworks.com/active-directory-certificate-se...	T3
	https://unit42.paloaltonetworks.com/npm-supply-chain-attack/	T3
CVE-2022-26923 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2022-26923	T1
CVE-2022-26923: Know Your AD Vulnerability	https://www.semperis.com/blog/ad-vulnerability-cve-2022-26923/	T3
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923	T1

Generated 2026-05-12 14:08 UTC by TJS Security Command Center