INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 18:45 UTC

CVE-2026-20929: Kerberos Relay via DNS CNAME Bypasses NTLM Mitigations, Enables Certificate-Based Persistence in AD Environments

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0050
Type	CVE Vulnerability
CVE ID	CVE-2026-20929
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0004 (14th percentile)
Affected Products	Microsoft Windows (Kerberos), Active Directory Certificate Services (AD CS), AD CS Web Enrollment (/certsrv endpoint)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CVE-2026-20929 allows attackers who can manipulate DNS records to relay Kerberos authentication to Active Directory Certificate Services, bypassing environments where NTLM has been disabled as a relay defense. Successful exploitation produces attacker-controlled certificates valid for a year or more, granting persistent, credential-independent access to Windows infrastructure. Microsoft patched this in January 2026; unpatched Active Directory environments with AD CS Web Enrollment enabled are at elevated risk of durable, difficult-to-detect compromise.

Technical Analysis

CVE-2026-20929 (CVSS 7.5, CWE-346/CWE-295/CWE-290) affects Microsoft Windows Kerberos and Active Directory Certificate Services (AD CS), specifically the Web Enrollment endpoint (/certsrv). The attack exploits DNS CNAME manipulation to control Service Principal Name (SPN) resolution, enabling an adversary-in-the-middle position (T1557) that relays Kerberos authentication to AD CS. This bypasses NTLM-relay defenses entirely since the relay operates over Kerberos. Once relay is achieved, the attacker requests a certificate via the AD CS issuance workflow (T1649). Resulting certificates are valid for one year or more and can be used for pass-the-ticket attacks (T1550.003) without requiring domain credentials. This is

functionally a Kerberos-based variant of the ESC8 attack chain, extending it to NTLM-hardened environments. DNS abuse is tracked under T1071.004. Microsoft patched this in the January 2026 Patch Tuesday release. NVD entry and Microsoft Security Advisory are available at the T1 sources listed in the item. EPSS score is 0.045% as of configuration date (indicating exploitation probability below 0.1%), placing it in the 13th percentile. This suggests limited observed exploitation in the wild at this time.

Action Checklist

1. Step 1: Containment. Apply the January 2026 Microsoft Patch Tuesday update addressing CVE-2026-20929 to all Windows domain controllers and systems running AD CS. Verify patch application via the Microsoft Security Response Center advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20929. Temporarily disable the AD CS Web Enrollment endpoint (/certsrv) on internet-facing or network-edge AD CS servers until patching is confirmed, or apply Extended Protection for Authentication (EPA) if disabling is not operationally feasible. Consult with infrastructure and CA teams to assess impact on legitimate enrollment workflows.
2. Step 2: Detection. Review DNS server logs for anomalous CNAME record creation or modification, particularly records pointing to attacker-controlled hosts or resolving to unexpected IP addresses. Query AD CS issuance logs (Event ID 4886 and 4887 on the CA) for certificates issued to accounts that do not typically request certificates, or for certificates issued via the Web Enrollment interface from unusual source IPs. Review Kerberos service ticket events (Event ID 4769) for TGS requests targeting the AD CS SPN from unexpected principals.
3. Step 3: Eradication. Apply the January 2026 Microsoft security update as the primary remediation. Additionally, enforce Extended Protection for Authentication (EPA) on the AD CS Web Enrollment IIS endpoint, which mitigates channel-binding bypass conditions. Audit DNS zone permissions to restrict unauthorized CNAME record creation; limit DNS write access to designated administrators only.
4. Step 4: Recovery. After patching, audit all certificates issued by your CA in the 90 days preceding patch application. Revoke any certificates issued to unexpected principals or via anomalous Web Enrollment requests. Verify CRL (Certificate Revocation List) distribution points are functional and that clients are enforcing revocation checks. Monitor AD CS Event IDs 4886, 4887, and 4888 for continued anomalous issuance activity for at least 30 days post-remediation.
5. Step 5: Post-Incident. This vulnerability exposes a control gap where NTLM relay mitigations were assumed to cover relay-based AD CS attack chains. Review your AD CS hardening posture against the full ESC attack surface (ESC1 through ESC8 and beyond), using MITRE T1649 as a hunting anchor. Evaluate whether AD CS Web Enrollment is required or can be replaced with a less attack-exposed enrollment method. Document DNS zone permission controls as a standing audit item.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal counsel if Event ID 4887 records confirm certificates were issued to privileged AD principals (Domain Admins, Enterprise Admins, service accounts with DCSync rights) via anomalous Web Enrollment requests, as this constitutes credential-independent persistent access to the AD forest and may trigger breach notification obligations under applicable data protection regulations if privileged access was leveraged against systems holding PII or PHI.
Recovery Notes	Post-containment recovery for CVE-2026-20929 centers on PKI integrity restoration: every certificate issued via the compromised /certsrv relay path must be treated as attacker-controlled and revoked, and CRL propagation must be verified to all clients before considering remediation complete. Monitor AD CS Event IDs 4886, 4887, and 4888 daily for a minimum of 30 days post-patch to detect any renewed relay attempts against the patched endpoint or pivot attempts against other enrollment interfaces. If any revoked certificate was tied to a computer or user account used for privileged access, rotate all associated credentials and Kerberos tickets (run `klist purge` on affected hosts and reset account passwords) since the attacker may have used the certificate for PKINIT-based authentication to obtain a TGT independently of the credential.
Forensic Artifacts	AD CS Security Event Log (evtx) from the CA server — Event IDs 4886 (request received), 4887 (certificate issued), 4888 (request denied): captures requester UPN, certificate template, and the source IP of the Web Enrollment relay request; the relayed Kerberos session would appear as a machine or service account UPN authenticating from an unexpected IP not associated with that account's normal workstation. | IIS W3C access logs from %SystemDrive%\inetpub\logs\LogFiles\W3SVC* on the AD CS Web Enrollment server: POST requests to /certsrv/certfnsh.asp with HTTP 200 responses indicate successful certificate issuance via Web Enrollment; the attacker's relay tool (e.g., krbrelayx) would generate these requests with a Kerberos Authorization header (WWW-Authenticate: Negotiate) sourced from a host IP inconsistent with the authenticated principal. | DNS Server Audit Event Log (Microsoft-Windows-DNSServer/Audit, Event ID 541) on all AD-integrated DNS servers: records dynamic DNS record additions and modifications including CNAME record creation; the relay prerequisite for CVE-2026-20929 requires a CNAME pointing a name resolvable by the CA to an attacker-controlled host, leaving a creation event with the attacker's source IP and the injected CNAME record value. | Windows Security Event ID 4769 (Kerberos Service Ticket Request) on domain controllers: TGS requests where the Service Name matches the AD CS host SPN (e.g., 'host/$') from a Client Address that is not a known admin workstation or enrollment system indicates a relay tool requesting a Kerberos ticket for the CA service as a precursor to the relay; ticket encryption type 0x17 (RC4) in these events is an additional relay indicator. | AD CS database certificate store — accessible via `certutil -view`: the issued certificates table contains the full certificate chain, SAN extensions, and requester metadata for every certificate the CA has ever issued; attacker-obtained certificates for privileged principals would appear here with NotBefore timestamps correlating to the relay window and template names associated with client authentication (e.g., 'User', 'Machine', 'DomainController', or any ESC1-vulnerable custom template with CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT).

Per-Action IR Details

Step 1: Containment — Apply the January 2026 Microsoft Patch Tuesday update addressing CVE-2026-20929 to all Windows domain controllers and systems running AD CS. Verify patch application via the Microsoft Security Response Center advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20929. Temporarily disable the AD CS Web Enrollment endpoint (/certsrv) on internet-facing or network-edge AD CS servers until patching is confirmed.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality) — disable /certsrv endpoint to reduce attack surface, CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If patch cannot be applied immediately, disable the AD CS Web Enrollment IIS application pool via PowerShell on the CA server: `Stop-WebAppPool -Name 'DefaultAppPool'; Set-WebConfiguration '/system.applicationHost/sites/site[@name="Default Web Site"]/application[@path="/certsrv"]' -Value @{enabled='false'}`. For domain controllers not yet patched, restrict inbound TCP 88 (Kerberos) from non-domain-joined hosts using Windows Firewall with Advanced Security: `New-NetFirewallRule -DisplayName 'Block External Kerberos' -Direction Inbound -Protocol TCP -LocalPort 88 -RemoteAddress -Action Block`. Validate patch KB installation across all DCs with: `Get-HotFix | Where-Object {$_.HotFixID -eq ''}` run via PsExec against each DC.

Evidence: Before applying the patch or disabling /certsrv, capture: (1) IIS access logs from the AD CS Web Enrollment server at %SystemDrive%\inetpub\logs\LogFiles\W3SVC* — preserve all logs from 90 days prior, filtering for POST requests to /certsrv/certfnsh.asp which indicate certificate requests submitted via Web Enrollment; (2) a live memory image of the CA server process (certsvc) using WinPmem or Magnet RAM Capture before any service restarts; (3) current DNS zone exports for all AD-integrated zones via `Export-DnsServerZone` to preserve the pre-remediation CNAME record state as forensic baseline; (4) the AD CS database snapshot via `certutil -backupdb ` to preserve the issuance record before any revocation actions alter it.

Step 2: Detection — Review DNS server logs for anomalous CNAME record creation or modification, particularly records pointing to attacker-controlled hosts or resolving to unexpected IP addresses. Query AD CS issuance logs (Event ID 4886 and 4887 on the CA) for certificates issued to accounts that do not typically request certificates, or for certificates issued via the Web Enrollment interface from unusual source IPs. Review Kerberos service ticket events (Event ID 4769) for TGS requests targeting the AD CS SPN from unexpected principals.

NIST Phase: Detection Analysis

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

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

Compensating: Without a SIEM, run the following on the CA server to extract Event ID 4886 (certificate request received) and 4887 (certificate issued) from the Security log, correlating requester account and source IP: `Get-WinEvent -ComputerName -FilterHashtable @{LogName='Security'; Id=4886,4887} | Select-Object TimeCreated, Message | Export-Csv C:\IR\adcs_issuance.csv`. On DNS servers, enable DNS debug logging via `dnscmd /config /log 8192` and parse the resulting DNS.log at %SystemRoot%\System32\dns\dns.log for CNAME record additions (record type 5) using: `Select-String -Path 'C:\Windows\System32\dns\dns.log' -Pattern 'CNAME'`. For Kerberos TGS Event ID 4769 analysis on DCs, filter for Service Name matching the AD CS SPN (typically 'host/'): `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4769} | Where-Object {$_.Message -match ''}`. Deploy the free Sigma rule for AD CS abuse (sigma rule 'win_security_adcs_certificate_request_unusual') using sigmac converted to PowerShell or Hayabusa for offline log analysis.

Evidence: Preserve before analysis to avoid log rotation loss: (1) The CA Security Event Log in evtx format — `wevtutil epl Security C:\IR\CA_Security.evtx` — capturing Event IDs 4886, 4887, and 4888 (certificate denied) which record requester UPN, template name, and request disposition; (2) DNS Server debug log and DNS Audit event log (Microsoft-Windows-DNSServer/Audit, Event ID 541 for dynamic record updates) from all DNS servers covering 90 days prior — CNAME records injected for this relay would appear as unexpected additions in zone records pointing the AD CS server name to an attacker-controlled IP; (3) IIS W3C logs from the /certsrv virtual directory on the AD CS Web Enrollment server, specifically POST requests to /certfnsh.asp, which carry the relayed Kerberos ticket and certificate template selection; (4) Windows Security Event ID 4769 from all domain controllers' Security logs filtered for TGS requests where the Service Name is the AD CS host SPN and the Client Address is an unexpected or non-administrative workstation IP.

Step 3: Eradication — Apply the January 2026 Microsoft security update as the primary remediation. Additionally, enforce Extended Protection for Authentication (EPA) on the AD CS Web Enrollment IIS endpoint, which mitigates channel-binding bypass conditions. Audit DNS zone permissions to restrict unauthorized CNAME record creation; limit DNS write access to designated administrators only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST SC-8 (Transmission Confidentiality and Integrity) — EPA enforces channel binding on IIS, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: To enforce EPA on the AD CS Web Enrollment IIS endpoint without enterprise tooling, run the following on the CA/IIS server to set Extended Protection to 'Required' on the /certsrv application: `Set-WebConfigurationProperty -Filter 'system.webServer/security/authentication/windowsAuthentication' -Name extendedProtection.tokenChecking -Value Require -PSPath 'IIS:\Sites\Default Web Site\certsrv'`. Verify the setting was applied: `Get-WebConfigurationProperty -Filter 'system.webServer/security/authentication/windowsAuthentication' -Name extendedProtection.tokenChecking -PSPath 'IIS:\Sites\Default Web Site\certsrv'`. For DNS zone permission hardening, use `Get-Acl -Path 'AD:\DC=,CN=MicrosoftDNS,DC=ForestDnsZones,DC=,DC='` to enumerate current ACEs, then remove non-admin write permissions using the AD module's `Set-Acl`. Document all ACE changes for the audit trail.

Evidence: Before executing eradication steps, capture the pre-hardening IIS authentication configuration for the /certsrv application as evidence of the misconfiguration that enabled relay: `appcmd list config 'Default Web Site/certsrv' /section:windowsAuthentication > C:\IR\certsrv_auth_config_prechange.txt`. Export DNS zone ACLs in their current vulnerable state: `(Get-Acl -Path 'AD:\DC=,CN=MicrosoftDNS,DC=ForestDnsZones,DC=,DC=').Access | Export-Csv C:\IR\dns_zone_acls_prechange.csv`. This documents the control gap that permitted the CNAME manipulation enabling Kerberos relay to AD CS.

Step 4: Recovery — After patching, audit all certificates issued by your CA in the 90 days preceding patch application. Revoke any certificates issued to unexpected principals or via anomalous Web Enrollment requests. Verify CRL (Certificate Revocation List) distribution points are functional and that clients are enforcing revocation checks. Monitor AD CS Event IDs 4886, 4887, and 4888 for continued anomalous issuance activity for at least 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity) — verify CA integrity post-remediation, NIST AU-11 (Audit Record Retention), NIST SC-17 (Public Key Infrastructure Certificates) — certificate lifecycle management, CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Enumerate all certificates issued by the CA in the past 90 days using certutil: `certutil -view -restrict 'NotBefore>=' -out RequestID,RequesterName,CertificateTemplate,NotBefore,NotAfter,DispositionMessage csv > C:\IR\issued_certs_90d.csv`. Cross-reference RequesterName values against accounts expected to hold machine or user certificates — any service account, computer account, or user account not previously enrolled is a revocation candidate. Revoke suspicious certificates using: `certutil -revoke 3` (reason code 3 = keyCompromise) and immediately publish an updated CRL: `certutil -crl`. Verify CRL distribution point reachability from a domain-joined client: `certutil -verify -urlfetch `. For the 30-day monitoring window without SIEM, schedule a daily Task Scheduler job running the Event ID 4886/4887 PowerShell query above and mailing output to the IR team.

Evidence: Before revoking certificates, export the full AD CS database view for the 90-day window as the evidentiary record of what was issued: `certutil -backupdb C:\IR\CA_DB_backup`. For each candidate revocation certificate, extract and preserve the certificate file: `certutil -getkey C:\IR\suspect_cert_.cer` — this captures the public key and SAN fields that would reveal if an attacker enrolled a certificate for a privileged principal (e.g., a Domain Admin UPN) via the relay. Verify CRL publication timestamps in the CA database: `certutil -view -restrict 'RequestID=' -out CertificateHash,NotBefore,NotAfter,DispositionMessage` to establish the exact issuance timeline for incident

documentation.

Step 5: Post-Incident — This vulnerability exposes a control gap where NTLM relay mitigations were assumed to cover relay-based AD CS attack chains. Review your AD CS hardening posture against the full ESC attack surface (ESC1 through ESC8 and beyond), using MITRE T1649 as a hunting anchor. Evaluate whether AD CS Web Enrollment is required or can be replaced with a less attack-exposed enrollment method. Document DNS zone permission controls as a standing audit item.

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 CA-7 (Continuous Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Run Certify (free, open-source from SpecterOps) against your AD CS environment to enumerate all ESC1–ESC8 misconfigurations: `Certify.exe find /vulnerable` — this identifies certificate templates with dangerous flags (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT for ESC1, overly permissive enrollment ACLs for ESC2, etc.) without requiring any enterprise tooling. For MITRE T1649 (Steal or Forge Authentication Certificates) hunting, deploy the free Sigma rule set from SigmaHQ targeting AD CS abuse (search SigmaHQ repository for 'adcs' or 'certificate') and run via Hayabusa against collected evtx files: `hayabusa csv-timeline -d C:\IR\evtx_archive -r sigma\rules\windows\builtin\security`. Document the decision to retain or decommission AD CS Web Enrollment (/certsrv) in your risk register, noting that ADCS certificate enrollment via RPC (DCOM) or autoenrollment via Group Policy does not expose the HTTP-based relay surface that CVE-2026-20929 exploits.

Evidence: Compile the full lessons-learned artifact package: (1) the pre-patch Certify ESC scan output documenting which ESC conditions existed at time of incident — this establishes the control gap baseline for the post-incident report; (2) DNS audit log exports showing the full timeline of CNAME record changes in affected zones for the 90-day window, which establishes attacker dwell time and manipulation scope; (3) the complete issued certificate roster from the CA DB backup with revocation actions documented — this serves as the PKI integrity attestation for any regulatory or leadership reporting obligations; (4) the pre- and post-hardening IIS EPA configuration exports for /certsrv as evidence of control implementation.

Detection Guidance

Primary detection surface is AD CS and DNS logs. On the CA server, monitor Event IDs 4886 (certificate request received) and 4887 (certificate issued) for requests originating from unexpected source hosts or accounts, particularly service accounts or machine accounts not enrolled in certificate-based auth workflows. On domain controllers, monitor Event ID 4769 (Kerberos service ticket request) for TGS requests targeting AD CS SPNs from atypical principals or source IPs. In DNS infrastructure, alert on CNAME record creation or modification in AD-integrated DNS zones by non-administrative accounts, query DNS audit logs (Event ID 770x in Windows DNS Server) for unauthorized zone record changes. Behavioral indicator: a certificate issued via /certsrv to a principal that has no documented business need for certificate-based authentication. Correlated indicator: DNS CNAME change followed within a short window by a Kerberos TGS request and a subsequent AD CS certificate issuance event for the same or related account. No confirmed public IOCs (IPs, hashes, domains) are available for this CVE at this time; detection relies on behavioral and event-log patterns rather than static indicators.

Framework Mappings

MITRE-ATTACK

- **T1557.001** — LLMNR/NBT-NS Poisoning and SMB Relay
- **T1558** — Steal or Forge Kerberos Tickets
- **T1649** — Steal or Forge Authentication Certificates
- **T1550.003** — Pass the Ticket
- **T1556.006** — Multi-Factor Authentication
- **T1071** — Application Layer Protocol
- **T1557** — Adversary-in-the-Middle
- **T1558.003** — Kerberoasting
- **T1071.004** — DNS

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	Credential-Access
T1558	Steal or Forge Kerberos Tickets	Credential-Access
T1649	Steal or Forge Authentication Certificates	Credential-Access
T1550.003	Pass the Ticket	Defense-Evasion
T1556.006	Multi-Factor Authentication	Credential-Access
T1071	Application Layer Protocol	Command-And-Control
T1557	Adversary-in-the-Middle	Credential-Access
T1558.003	Kerberoasting	Credential-Access
T1071.004	DNS	Command-And-Control

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/detecting-kerberos-relay-att...	T3
	https://cyberpress.org/poc-for-kerberos-relay-attack/	T3
	https://cybersecuritynews.com/kerberos-relay-attack-uses-dns-cname/	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-id-brings...	T3
CVE-2026-20929 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-20929	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20929	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-17 18:45 UTC by TJS Security Command Center