INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-01 13:38 UTC

CVE-2026-41089: Windows Netlogon Critical RCE Actively Exploited, Domain Controllers at Risk

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0248
Type	CVE Vulnerability
CVE ID	CVE-2026-41089
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0009 (26th percentile)
Affected Products	Microsoft Windows (Netlogon service), specific affected versions not confirmed from available sources; domain controllers identified as primary target
Published	3 hours ago
Discovery Source	Serper

Executive Summary

A critical remote code execution vulnerability in the Windows Netlogon service is being actively exploited in the wild, with domain controllers identified as the primary target. Netlogon is the authentication backbone of Active Directory environments; a successful exploit grants an attacker the ability to execute arbitrary code on domain controllers, potentially seizing control of an entire Windows domain. Organizations running Windows domain infrastructure should treat this as an emergency patching event, full domain compromise is the realistic worst-case outcome.

Technical Analysis

CVE-2026-41089 is a critical RCE in the Windows Netlogon service, the protocol responsible for authenticating users and machines in Active Directory domains. The vulnerability is network-accessible with no authentication required, consistent with CVSS base score of 9.8. Active exploitation in the wild has been reported via security press. MITRE ATT&CK techniques associated with this vulnerability include T1210 (Exploitation of Remote Services), T1078.002 (Valid Accounts: Domain Accounts), and T1068 (Exploitation for Privilege Escalation). CWE classification has not been confirmed from primary sources; refer to NVD for authoritative CWE mapping. Affected Windows versions have not been independently confirmed from NVD or MSRC within this session; consult https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089 and https://nvd.nist.gov/vuln/detail/cve-2026-41089 for authoritative scope and patch details. CVSS vendor score not

yet published by NVD; score may be refined when vendor-supplied CVSS data becomes available. EPSS score is 0.095% (26th percentile), indicating below-median likelihood of exploitation in the wild; however, security press reports indicate active exploitation, suggesting a potential reporting lag in EPSS data. Organizations should not rely solely on EPSS for prioritization when public exploitation is confirmed. CISA KEV listing not confirmed at time of report generation.

Action Checklist

1. Step 1: Containment. Immediately restrict inbound Netlogon RPC traffic (TCP/UDP 135 and ephemeral ports 49152-65535) to domain controllers, limiting access to internal administrative networks only. In parallel, confirm patch availability via MSRC at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089. Apply the Microsoft security update on an emergency basis to all domain controllers within 24 hours. Isolate any domain controller showing anomalous behavior pending investigation. Reference NIST SI-4 (System Monitoring) to verify logging is active on affected systems before patching.
2. Step 2: Detection. Query Windows Security Event Log on all domain controllers for anomalous Netlogon activity: Event ID 5805 (Netlogon: failed DC locator call, may indicate failed Netlogon communication), Event ID 4625 (failed logon), and Event ID 4742 (computer account changed). Review Netlogon.log (default path: %SystemRoot%\debug\netlogon.log) for unexpected session establishment attempts from unknown sources. Build SIEM correlation rules: detect privilege escalation events (Event ID 4672, 4673) occurring within 5 minutes of unusual Netlogon activity (5805, 4625) from the same source IP. Reference NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) to confirm logging is enabled across all domain controllers.
3. Step 3: Eradication. Apply the Microsoft security update for CVE-2026-41089 to all domain controllers immediately; consult the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089 for the specific KB article and patch ID. After patching, rotate the KRBTGT account password twice in sequence per Microsoft documented procedure (refer to official Microsoft guidance or https://learn.microsoft.com/en-us/windows-server for KRBTGT reset steps) to invalidate any Kerberos tickets that may have been issued under a compromised domain context. Apply credential rotation procedures for all domain administrator accounts. Reference NIST SI-2 (Flaw Remediation) and CIS 7.3 (Perform Automated Operating System Patch Management).
4. Step 4: Recovery. Validate patch deployment across all domain controllers using your patch management console; confirm Event ID 19 installation events on each DC, cross-referencing the KB article number from the MSRC advisory to ensure the correct patch was applied. Re-enable any isolated domain controllers only after patch confirmation. Monitor Netlogon.log and SIEM for 72 hours post-patch for residual anomalous authentication activity. Verify domain controller integrity using NIST SI-7 (Software, Firmware, and Information Integrity), checking for unauthorized changes to system binaries, services, and scheduled tasks. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-remediation review cadence.
5. Step 5: Post-Incident. Assess whether your domain controller tier had Netlogon RPC exposure to untrusted network segments, and close that gap permanently via firewall segmentation (CIS 4.4, Implement and Manage a Firewall on Servers). Review privileged account access scope against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Evaluate whether domain controllers are enrolled in a privileged access workstation (PAW)

model. Monitor event logs for newly created or modified local administrator accounts on domain controllers, which may indicate post-exploitation persistence (NIST SI-4, System Monitoring). Document findings for the next scheduled audit cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior leadership, legal, and (if applicable) regulatory counsel immediately if any of the following are confirmed: (1) Event ID 4742 shows unauthorized computer account modification indicating domain object manipulation post-exploitation; (2) KRBTGT PasswordLastSet predates the incident window but Kerberos golden ticket artifacts are detected in memory or logs, indicating potential pass-the-ticket lateral movement to additional systems containing PII, PHI, or PCI-scoped data that may trigger breach notification obligations; (3) the organization lacks the in-house capability to perform KRBTGT rotation and AD integrity validation, requiring engagement of an external DFIR retainer.
Recovery Notes	Before returning any isolated domain controller to production, confirm patch installation via `Get-HotFix`, validate ntds.dit and Netlogon service binary integrity via SHA-256 hash comparison against a clean peer DC, and verify AD replication health with `repadmin /replsummary` to ensure no attacker-modified AD objects are propagating. Maintain elevated monitoring of Netlogon.log, Windows Security Event Log (Event IDs 5805, 4742, 4672, 4673), and Kerberos TGT issuance patterns for a minimum of 72 hours post-patch across all domain controllers. If any anomalous Netlogon session negotiation or unexpected privileged ticket issuance is observed during the monitoring window, treat the environment as not fully eradicated and re-initiate containment.
Forensic Artifacts	Netlogon.log (%SystemRoot%\debug\netlogon.log) — this file records all Netlogon RPC session negotiations; CVE-2026-41089 exploitation of the Netlogon service RPC interface would produce malformed or unexpected session entries from non-DC source IPs immediately prior to any observed privilege escalation, making this the primary exploitation timing artifact. | Windows Security Event Log EVTX — specifically the sequence of Event ID 5805 (Netlogon session setup failure from an unexpected machine account) followed within seconds by Event ID 4742 (computer account changed) and Event ID 4672/4673 (special privileges assigned to new logon) from the same source, which maps to the exploitation-to-privilege-escalation kill chain for a Netlogon RCE targeting domain controllers. | Active Directory ntds.dit database (%SystemRoot%\NTDS\ntds.dit) — an attacker achieving RCE on a domain controller via CVE-2026-41089 has the capability to write directly to the AD database; SHA-256 hash comparison of ntds.dit against a verified clean DC and forensic parsing with a tool such as ntdsextract or impacket's secretsdump (in offline mode against a VSS snapshot) can reveal unauthorized account creation, privilege grants, or SID history injection. | Registry key HKLM\SYSTEM\CurrentControlSet\Services\Netlogon — post-RCE persistence on a domain controller frequently involves modifying the Netlogon service ImagePath or adding a malicious DLL via the service's DependOnService or ServiceDll parameters; export and diff this key against a known-good baseline to detect service hijacking introduced during the exploitation window. | Windows System Event Log entries for Event ID 7045 (A new service was installed) and Security Event Log Event ID 4697 (A service was installed in the system) — RCE on the Netlogon service grants SYSTEM-level access on a domain controller, which is commonly leveraged to install a persistence service or scheduled task; these event IDs timestamped within the exploitation window are high-fidelity indicators of post-exploitation persistence specific to this attack class.

Per-Action IR Details

Step 1: Containment — Immediately restrict inbound Netlogon traffic (TCP/UDP 135, 49152–65535 RPC dynamic ports) to domain controllers from untrusted network segments. Confirm patch availability via MSRC at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089 and apply on an emergency basis to all domain controllers before broader fleet deployment. Isolate any domain controller showing anomalous behavior pending investigation. Reference NIST SI-4 (System Monitoring) to verify logging is active on affected systems before patching.

NIST Phase: Containment

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

Controls: NIST SI-4 (System Monitoring), NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On domain controllers without a host-based firewall policy managed via GPO, immediately run: `netsh advfirewall firewall add rule name='Block Netlogon RPC Untrusted' dir=in action=block protocol=TCP localport=135,49152-65535 remoteip=` — repeat for UDP. Deploy Sysmon with a config that captures network connection events (Event ID 3) on TCP/135 and dynamic RPC ports; filter for source IPs outside your DC-to-DC and trusted admin subnet ranges. Document the firewall rule and the timestamp of application as containment evidence.

Evidence: Before applying firewall rules or patches, capture: (1) `netstat -ano` output on each DC to record all active connections on TCP/135 and dynamic RPC ports — note any source IPs that are not peer DCs or known admin hosts; (2) Netlogon.log at %SystemRoot%\debug\netlogon.log — preserve a read-only copy; RCE exploitation of the Netlogon service may produce malformed session negotiation entries immediately prior to the anomalous behavior; (3) Windows Security Event Log entries for Event ID 5805 (Netlogon session setup failure with unexpected machine accounts) and Event ID 4742 (computer account modification) timestamped within the exploitation window; (4) Running process list (`tasklist /svc`) and service state of the Netlogon service (`sc query netlogon`) to identify any injected or substitute service binary.

Step 2: Detection — Query Windows Security Event Log on all domain controllers for anomalous Netlogon activity: Event ID 5805 (Netlogon session setup failure), Event ID 4625 (failed logon), and Event ID 4742 (computer account changed). Review Netlogon.log (default path: %SystemRoot%\debug\netlogon.log) for unexpected session establishment attempts from unknown sources. Alert on lateral movement patterns consistent with T1210 and T1068 — specifically privilege escalation events (Event ID 4672, 4673) following Netlogon activity from non-administrative hosts. Reference NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) to confirm logging is enabled across all domain controllers.

NIST Phase: Detection Analysis

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

Controls: 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), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, run this PowerShell one-liner on each DC to extract and correlate the relevant events: `Get-WinEvent -ComputerName -FilterHashtable @{LogName='Security'; Id=5805,4625,4742,4672,4673; StartTime=(Get-Date).AddDays(-7)} | Select-Object TimeCreated,Id,Message | Export-Csv C:\IR\netlogon_events.csv -NoTypeInformation`. Cross-reference CSV timestamps: look for Event ID 4672 or 4673 (special privileges assigned) appearing within 60 seconds of a 5805 or 4742 from the same source IP — that sequence maps to MITRE T1068 (Exploitation for Privilege Escalation) chained with T1210 (Exploitation of Remote Services) via the Netlogon RPC path. For real-time alerting, deploy the free Sigma rule targeting Netlogon anomalies (search sigma-rules GitHub for 'win_netlogon') and convert to Windows Event Forwarding (WEF) subscriptions.

Evidence: Before concluding the detection phase, preserve: (1) Full Netlogon.log content — RCE exploitation of the Netlogon service RPC interface would produce entries showing unexpected machine account names, malformed credential validation sequences, or session establishments from IPs not in the domain's known DC or member server inventory; (2) Windows Security Event Log export (EVTX format) covering the full 7-day window prior to detection for all

four event IDs (5805, 4625, 4742, 4672/4673); (3) Active Directory replication metadata for any computer account modified during the window — run `repadmin /showobjmeta 'CN=,CN=Computers,DC=domain,DC=com'` to detect unauthorized account manipulation consistent with MITRE T1210 post-exploitation; (4) Sysmon Event ID 3 (Network Connection) logs filtered for lsass.exe or svchost.exe (hosting Netlogon) making outbound connections to non-DC hosts, which would indicate post-compromise lateral movement.

Step 3: Eradication — Apply the Microsoft security update for CVE-2026-41089 to all domain controllers immediately; consult the MSRC advisory for the specific KB article and patch ID (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089). After patching, rotate the KRBTGT account password twice in sequence per Microsoft documented procedure to invalidate any Kerberos tickets that may have been issued under a compromised domain context. Apply D3-CRO (Credential Rotation) for all domain administrator accounts. Reference NIST SI-2 (Flaw Remediation) and CIS 7.3 (Perform Automated Operating System Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without an enterprise patch management console: download the specific KB identified in the MSRC advisory for CVE-2026-41089, stage it on an internal file share, then push via: `wusa.exe \\fileserver\patches\.msu /quiet /norestart` executed through a scheduled task or PSExec against each DC sequentially, starting with non-FSMO-role DCs. For KRBTGT rotation without privileged tooling, use the Microsoft-provided KRBTGT Account Password Reset Script (available on Microsoft's GitHub — verify the URL at time of download): run it twice with a minimum 10-hour gap to ensure replication convergence and Kerberos ticket expiry across all DCs. Confirm rotation by checking `Get-ADUser krbtgt -Properties PasswordLastSet`.

Evidence: Before patching and credential rotation, capture: (1) Output of `Get-ADUser krbtgt -Properties PasswordLastSet, WhenChanged` to establish the KRBTGT password age baseline — an unexpectedly recent change would indicate the attacker already rotated it (indicating full domain compromise requiring forest-level recovery); (2) List of all currently active Kerberos TGTs using `klist sessions` on each DC and from privileged admin workstations, noting any tickets issued to accounts that were not explicitly authorized to authenticate during the suspected exploitation window; (3) Full registry export of `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon` from each DC to document service binary path and parameters — an attacker with RCE on the Netlogon service may have modified the ImagePath or injected a DLL; (4) Hash of the Netlogon service binary (`Get-FileHash C:\Windows\System32\netlogon.dll -Algorithm SHA256`) compared against a known-good value from an unaffected system running the same OS build.

Step 4: Recovery — Validate patch deployment across all domain controllers using your patch management console; confirm Event ID 19 (Windows Update successful install) on each target. Re-enable any isolated domain controllers only after patch confirmation. Monitor Netlogon.log and SIEM for 72 hours post-patch for residual anomalous authentication activity. Verify domain controller integrity using D3-SFA (System File Analysis) — check for unauthorized changes to system binaries, services, and scheduled tasks. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-remediation review cadence.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without a patch management console, validate via PowerShell on each DC: `Get-HotFix -Id ` — absence of the KB confirms the patch did not apply. For system integrity verification without a commercial tool, run `sfc /scannow` on each DC post-patch and review CBS.log at `%SystemRoot%\Logs\CBS\CBS.log` for any replaced or

flagged system files related to the Netlogon service stack. Check scheduled tasks for persistence using: `schtasks /query /fo LIST /v | findstr /i 'netlogon lsass rpc'`. Monitor Netlogon.log by tailing it with a PowerShell loop: `Get-Content %SystemRoot%\debug\netlogon.log -Wait` — watch for session negotiation entries from any IP added to your containment watchlist.

Evidence: Before re-introducing isolated DCs to production: (1) Run `Get-FileHash` against netlogon.dll, lsass.exe, and ntds.dit (the Active Directory database at `%SystemRoot%\NTDS\ntds.dit`) on the returning DC and compare hashes to a verified clean DC at the same patch level — ntds.dit modification would indicate the attacker wrote to the AD database during the compromise window; (2) Review Windows System Event Log for Event ID 7045 (new service installed) and Event ID 4697 (service installed in the security log) within the exploitation window — RCE on a DC commonly results in a persistence service being registered; (3) Export and diff the `HKLM\SYSTEM\CurrentControlSet\Services` registry hive against a known-good baseline to detect any new or modified service entries introduced via the Netlogon RCE; (4) Confirm AD replication health with `repadmin /replsummary` to ensure the returning DC is not replicating attacker-introduced changes to the domain partition.

Step 5: Post-Incident — Assess whether your domain controller tier had Netlogon RPC exposure to untrusted network segments, and close that gap permanently via firewall segmentation (CIS 4.4 — Implement and Manage a Firewall on Servers). Review privileged account access scope against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Evaluate whether domain controllers are enrolled in a privileged access workstation (PAW) model. Document findings for the next scheduled audit cycle.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST CA-7 (Continuous Monitoring), NIST RA-3 (Risk Assessment), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: To assess historical Netlogon RPC exposure without a network monitoring platform, pull Windows Firewall logs from each DC (`%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`) and filter for ALLOW entries on ports 135 and 49152–65535 from IPs outside your trusted DC and admin subnet ranges — this reconstructs pre-incident exposure. For PAW model evaluation on a budget, implement a Group Policy Object that restricts interactive logon to DCs (`User Rights Assignment → Allow log on locally`) to a dedicated admin group, and enforces `Deny access to this computer from the network` for all standard user accounts on DC OUs — this approximates PAW segmentation without dedicated hardware.

Evidence: For the post-incident lessons-learned record: (1) Compile the full timeline of Event IDs 5805, 4742, 4672/4673 correlated against network firewall logs to establish the attacker's dwell time between initial Netlogon exploitation and first observed privilege escalation — this dwell time metric directly informs detection gap remediation; (2) Document the network path that permitted RPC traffic from untrusted segments to reach the DC, including any firewall rule exceptions or missing micro-segmentation that enabled the attack surface for CVE-2026-41089; (3) Produce an account audit report showing which domain administrator accounts were active, their last authentication timestamps, and whether any were used from non-PAW hosts during the incident window, using `Get-ADUser -Filter {AdminCount -eq 1} -Properties LastLogonDate, DistinguishedName`.

Detection Guidance

Primary detection surface is the Windows Security Event Log and Netlogon debug log on domain controllers. Key event IDs: 5805 (Netlogon channel setup issue, may indicate failed exploit attempts), 4625 (failed logon with unusual source IPs), 4742 (computer account modification, potential post-exploitation), 4672 (special privileges assigned at logon, potential privilege escalation post-exploit), 4673 (privileged service called). Enable Netlogon debug logging if not already active (nltest /dbflag:0x2080ffff). In your SIEM, build a correlation rule: Netlogon-related events from a single source IP exceeding a threshold within a short window, combined with

subsequent 4672 events from the same source. Cross-reference source IPs against known internal domain controller IP ranges; unexpected Netlogon session establishment from workstation subnets or external IPs is a strong indicator. At time of report generation, no public IOC feeds (IP addresses, domains, file hashes) were available for this vulnerability. Organizations should monitor vendor security advisories and threat intelligence feeds (CISA, VulnCheck, Shadowserver) for IOC releases. When available, ingest IOCs into SIEM and firewall systems. Monitor event logs for newly created or modified local administrator accounts on domain controllers, which may indicate post-exploitation persistence. Reference NIST AU-12 (Audit Record Generation) and CIS 8.2 (Collect Audit Logs) to confirm DC logging posture.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1078.002** — Domain Accounts
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IR-5** — Incident Monitoring

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1210	Exploitation of Remote Services	Lateral-Movement
T1078.002	Domain Accounts	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
	https://www.helpnetsecurity.com/2026/06/01/windows-netlogon-rce-exp...	T3
(consolidated)	https://www.bleepingcomputer.com/news/microsoft/critical-windows-ne...	T3

Source	URL	Tier
Microsoft Security Update Guide: CVE-2026-41089	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089	**T1**
CVE-2026-41089 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-41089	**T1**
CVE-2026-41089 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-41089	**T3**