INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 14:02 UTC

Critical Windows Netlogon Vulnerability Under Active Exploitation, Patch Immediately

CVE VULNERABILITY | CRITICAL | CVSS 9.0

SCC Item ID	SCC-CVE-2026-0255
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	9.0
Affected Products	Windows Server (specific versions unconfirmed from available source data; likely broad Windows Server coverage based on Netlogon component scope)
Published	21 hours ago
Discovery Source	Serper

Executive Summary

A critical remote code execution vulnerability in the Windows Netlogon component is being actively exploited following Microsoft's May 2025 Patch Tuesday disclosure. Any unpatched Windows Server environment with Netlogon exposed is at immediate risk of full system compromise. Organizations that have not applied the May 2025 cumulative update should treat this as an emergency patching event.

Technical Analysis

A critical flaw in the Windows Netlogon component (CWE-94: Code Injection) allows unauthenticated or low-privilege remote code execution against affected Windows Server systems. The vulnerability maps to MITRE ATT&CK T1210 (Exploitation of Remote Services) and T1078.002 (Valid Accounts: Domain Accounts), suggesting attackers may chain exploitation with credential-based persistence. A CVSS base score of 9.0 reflects the severity. The CVE identifier is CVE-2025-59287. Active exploitation has been reported. The May 2025 Patch Tuesday cumulative update is the remediation vehicle. For the complete list of affected Windows Server versions, consult the official Microsoft Security Response Center (MSRC) advisory. CISA KEV status is pending confirmation.

Action Checklist

1. Step 1: Containment. Identify all Windows Server domain controllers. Prioritize the isolation of internet-facing or perimeter-exposed systems. If patching cannot occur within 24 hours, restrict inbound TCP 445 (SMB) and TCP 135 (RPC endpoint mapper) at the network perimeter to limit remote exploitation

surface (NIST SC-7: Boundary Protection). Verify that Netlogon traffic is not unnecessarily exposed outside the internal network.

2. Step 2: Detection. Query Windows Security event logs for anomalous Netlogon authentication activity: Event ID 5805 (Netlogon session setup failures), Event ID 4624/4625 (logon success/failure with unusual source IPs), and Event ID 4768/4769 (Kerberos ticket requests from unexpected hosts). Review LSASS access patterns for signs of credential dumping post-exploitation. Correlate with network logs for unexpected RPC or SMB traffic originating from non-standard hosts. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), ensure log collection is active on all domain controllers before investigating.

3. Step 3: Eradication. Apply the Microsoft May 2025 Patch Tuesday cumulative update to all Windows Server systems, prioritizing domain controllers. Verify patch installation using Windows Update history or WSUS/SCCM compliance reports. Confirm the Netlogon service is running the patched binary post-update. Per CIS 7.3 (Perform Automated Operating System Patch Management), automated patch deployment should be validated against all server tiers, not just Tier 0 assets.

4. Step 4: Recovery. After patching, restart the Netlogon service and confirm domain authentication is functioning normally across all domain-joined systems. Run a post-patch vulnerability scan against domain controllers to confirm the flaw is no longer present. Monitor Netlogon event logs (Event IDs 5805, 4624, 4768) for 72 hours post-remediation for signs of continued exploitation attempts or established persistence. Per NIST IR-4 (Incident Handling), document all actions taken and confirm no lateral movement occurred before clearing the incident.

5. Step 5: Post-Incident. Evaluate whether domain controllers have unnecessary internet exposure and remediate via network segmentation (NIST AC-4: Information Flow Enforcement, NIST SC-7). Review privileged account inventory against CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts); Netlogon RCE is most damaging when attackers have a path to domain admin. Implement or validate MFA on all administrative and remote access paths per CIS 6.5 (Require MFA for Administrative Access) and NIST AC-17 (Remote Access). Schedule a recurring Netlogon configuration review as part of your vulnerability management process (CIS 7.1).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if forensic evidence confirms successful exploitation — specifically: any Event ID 4720/4728 indicating attacker-created accounts, Sysmon Event ID 10 showing LSASS credential dumping, or AD replication metadata showing unauthorized schema or object changes — as successful Netlogon RCE against a domain controller constitutes full Active Directory compromise with likely regulatory breach notification obligations under HIPAA, PCI-DSS, and applicable state breach notification statutes.

Recovery Notes	Before returning domain controllers to full production status, verify AD integrity using `repadmin /replsummary` and `dcdiag /test:replications /test:kccevent` to confirm no replication anomalies were introduced during the exploitation window. Monitor Windows Security Event IDs 5805, 4624, 4768, and 4769 on all domain controllers for a minimum of 72 hours post-patch, with particular attention to authentication events from hosts that do not appear in the pre-incident asset inventory, as Netlogon RCE can enable attackers to forge machine account credentials and authenticate as non-existent systems. If any indicators of post-exploitation activity are confirmed (new accounts, modified GPOs, LSASS access), extend monitoring to 30 days and initiate a full Active Directory security assessment before clearing the incident.
Forensic Artifacts	Netlogon debug log (%SystemRoot%\debug\netlogon.log and netlogon.bak) — primary artifact for this vulnerability class; records all Netlogon session negotiations and will show anomalous machine account names, repeated secure channel setup failures (0xC0000022), or NO_CLIENT_SITE errors consistent with exploitation attempts against the Netlogon RPC interface | Windows Security Event Log on domain controllers — specifically Event IDs 5805 (Netlogon session setup failure), 4624/4625 (logon success/failure from unexpected source IPs), 4768/4769 (Kerberos TGT/service ticket requests from non-inventory hosts), and 4742 (computer account changed) which would indicate attacker manipulation of machine account attributes post-exploitation | LSASS memory and Sysmon Event ID 10 (ProcessAccess) logs — a successful Netlogon RCE granting SYSTEM or domain admin access would almost certainly be followed by credential dumping from LSASS; capture lsass.exe memory with Task Manager or ProcDump (`procdump -ma lsass.exe lsass.dmp`) before patching if exploitation is suspected, and preserve Sysmon logs showing GrantedAccess masks 0x1010 or 0x1fffff targeting lsass.exe | Active Directory replication metadata and object change audit (`repadmin /showchanges /verbose`) — a domain-level RCE via Netlogon provides attackers direct access to modify AD objects; this artifact will reveal unauthorized additions to privileged groups (Domain Admins, Enterprise Admins, Schema Admins), new computer or user account creation, or AdminSDHolder modifications used to establish covert persistent privileged access | Pre- and post-patch netlogon.dll file hash and version (`Get-FileHash C:\Windows\System32\netlogon.dll -Algorithm SHA256`) combined with Windows Update event log (System Event ID 19) — establishes forensic proof of the patch state at time of incident and confirms whether exploitation occurred against an already-patched or unpatched binary, which is critical for breach notification timeline determination

Per-Action IR Details

Step 1: Containment — Identify all Windows Server systems running the Netlogon service (domain controllers are highest priority). Isolate internet-facing or perimeter-exposed domain controllers immediately. Where patching cannot occur within 24 hours, consider restricting inbound TCP 445 and RPC endpoint mapper (TCP 135) at the network perimeter to limit remote exploitation surface (NIST SC-7: Boundary Protection). Verify no Netlogon traffic is unnecessarily exposed outside the internal network.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On each domain controller, run: `netstat -ano | findstr ':445 :135'` to enumerate active Netlogon/RPC listeners and identify unexpected external connections. Use Windows Firewall (`netsh advfirewall firewall add rule name='Block Netlogon External' dir=in protocol=tcp localport=135,445 remoteip=! action=block`) to block non-RFC1918 source IPs. On the network perimeter, if only a consumer-grade firewall is available, create an inbound deny rule for TCP 135 and TCP 445 from all WAN-facing interfaces. Document the change with a timestamp before

applying.

Evidence: Before isolating, capture a full netstat snapshot (`netstat -anob > C:\IR\netstat_pre_containment.txt`) to record any active RPC or SMB sessions to the domain controller at time of discovery. Collect the Netlogon debug log (`%SystemRoot%\debug\netlogon.log` and `netlogon.bak`) — this log records all Netlogon session negotiations and will show anomalous machine accounts or spoofed computer names indicative of exploitation. Export the System event log and Security event log from all domain controllers before any network changes alter active session state.

Step 2: Detection — Query Windows Security event logs for anomalous Netlogon authentication activity: Event ID 5805 (Netlogon session setup failures), Event ID 4624/4625 (logon success/failure with unusual source IPs), and Event ID 4768/4769 (Kerberos ticket requests from unexpected hosts). Review LSASS access patterns for signs of credential dumping post-exploitation. Correlate with network logs for unexpected RPC or SMB traffic originating from non-standard hosts. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), ensure log collection is active on all domain controllers before investigating.

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-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following on each domain controller using PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(5805,4624,4625,4768,4769)} | Select-Object TimeCreated,Id,Message | Export-Csv C:\IR\netlogon_events.csv`. For LSASS access patterns indicative of post-exploitation credential dumping, deploy Sysmon (Event ID 10 — ProcessAccess targeting lsass.exe) using SwiftOnSecurity's Sysmon config if not already present. Use the Sigma rule `win_lsass_access_non_system_account.yml` (SigmaHQ repository) converted to PowerShell-compatible XML for offline correlation. Parse the Netlogon debug log for repeated session setup failures from a single source IP: `Select-String -Path C:\Windows\debug\netlogon.log -Pattern '0xC0000022|0xC000006D|NO_CLIENT_SITE'`.

Evidence: Preserve the Netlogon debug log (`%SystemRoot%\debug\netlogon.log` and `netlogon.bak`) immediately — this is the primary artifact for this specific vulnerability class, as exploitation of a Netlogon RCE will generate abnormal session negotiation entries. Collect Sysmon Event ID 10 logs showing GrantedAccess masks of `0x1010` or `0x1fffff` against `lsass.exe`, which indicates credential dumping following a successful exploit. Export Windows Security Event IDs 4648 (explicit credential logon), 4672 (special privileges assigned), and 7045 (new service installed) from the domain controller Security log to identify post-exploitation privilege escalation or persistence mechanisms installed after Netlogon compromise.

Step 3: Eradication — Apply the Microsoft May 2025 Patch Tuesday cumulative update to all Windows Server systems, prioritizing domain controllers. Verify patch installation using Windows Update history or WSUS/SCCM compliance reports. Confirm the Netlogon service is running the patched binary post-update. Per CIS 7.3 (Perform Automated Operating System Patch Management), automated patch deployment should be validated against all server tiers — not just Tier 0 assets.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without WSUS or SCCM, verify patch installation per domain controller using: `Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 10` and cross-reference the KB number from the Microsoft May 2025 Patch Tuesday advisory for the Netlogon component. Confirm the patched `netlogon.dll` file version by running: `(Get-Item C:\Windows\System32\netlogon.dll).VersionInfo` and comparing the FileVersion against the version listed in the Microsoft Security Update Guide for this specific CVE. For environments using standalone Windows Update, run `wuauclt /detectnow /updatenow` or `UsoClient StartScan` on each server and confirm

completion via `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 19}` (Windows Update successful installation event).

Evidence: Before applying the patch, capture the current `netlogon.dll` file hash (`Get-FileHash C:\Windows\System32\netlogon.dll -Algorithm SHA256`) and record the pre-patch file version for forensic baseline documentation. If exploitation is suspected to have already occurred, acquire a full memory image of the domain controller using WinPmem (free, open-source) before rebooting for the patch, as reboot will destroy volatile evidence of any injected shellcode or in-memory implants that this Netlogon RCE may have delivered. Preserve the Windows Update log (`Get-WindowsUpdateLog`) post-patch to document the exact KB installed, timestamp, and success/failure status for chain-of-custody purposes.

Step 4: Recovery — After patching, restart the Netlogon service and confirm domain authentication is functioning normally across all domain-joined systems. Run a post-patch vulnerability scan against domain controllers to confirm the flaw is no longer present. Monitor Netlogon event logs (Event IDs 5805, 4624, 4768) for 72 hours post-remediation for signs of continued exploitation attempts or established persistence. Per NIST IR-4 (Incident Handling), document all actions taken and confirm no lateral movement occurred before clearing the incident.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CA-7 (Continuous Monitoring), NIST SI-6 (Security and Privacy Function Verification), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Confirm domain authentication health by running `nltest /sc_verify:` from a domain-joined member server — a successful secure channel verify confirms the Netlogon service is operating correctly post-patch. For the post-patch vulnerability scan without a commercial scanner, use the free Nessus Essentials (up to 16 IPs) targeting only domain controllers, or run `wmic qfe list` and compare against the Microsoft MSRC published KB for this Netlogon CVE. For the 72-hour monitoring window, schedule a recurring PowerShell job every 4 hours: `Get-WinEvent -LogName Security -MaxEvents 1000 | Where-Object {$_.Id -in @(5805,4624,4768)} | Export-Csv C:\IR\recovery_monitor_$(Get-Date -Format 'yyyyMMdd_HHmm').csv` to capture any resumed exploitation attempts.

Evidence: Before clearing the incident, collect and preserve the complete Active Directory replication metadata (`repadmin /showrepl * /csv > C:\IR\repl_post_recovery.csv`) to detect any unauthorized changes to domain objects that may indicate an attacker modified AD schema, added accounts, or established persistence via AdminSDHolder or group policy during the exploitation window. Review for new or modified scheduled tasks on domain controllers (`schtasks /query /fo CSV /v > C:\IR\scheduled_tasks_post_recovery.csv`) and new services (`Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045}`) that could represent backdoors installed via the Netlogon RCE before patching.

Step 5: Post-Incident — Evaluate whether domain controllers have unnecessary internet exposure and remediate via network segmentation (NIST AC-4: Information Flow Enforcement, NIST SC-7). Review privileged account inventory against CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — Netlogon RCE is most damaging when attackers have a path to domain admin. Implement or validate MFA on all administrative and remote access paths per CIS 6.5 (Require MFA for Administrative Access) and NIST AC-17 (Remote Access). Schedule a recurring Netlogon configuration review as part of your vulnerability management process (CIS 7.1).

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Audit privileged account exposure without commercial PAM tooling using: `Get-ADGroupMember 'Domain Admins' -Recursive | Select-Object Name,SamAccountName | Export-Csv C:\IR\domain_admins_audit.csv` and `Get-ADGroupMember 'Enterprise Admins' -Recursive | Select-Object Name,SamAccountName >> C:\IR\domain_admins_audit.csv` — any service accounts, non-Tier-0 admin accounts, or accounts with SPNs set in these groups represent paths an attacker could exploit post-Netlogon RCE. For free MFA on RDP administrative access without Azure AD Premium, deploy Duo Security's free tier (up to 10 users) or configure Windows Hello for Business with PIN complexity. For recurring Netlogon configuration review, create a monthly cron-equivalent scheduled task that runs `netlogon` service binary hash verification and compares against a known-good baseline.

Evidence: For lessons-learned documentation, retrieve the full Active Directory change audit trail for the exploitation window by querying Event ID 4720 (account created), 4728 (member added to global security group), 4732 (member added to local group), and 4756 (member added to universal group) from domain controller Security logs — these event IDs will reveal any persistence mechanisms an attacker may have established via the Netlogon RCE before containment. Export Group Policy Object version history (`Get-GPO -All | Select-Object DisplayName,ModificationTime | Sort-Object ModificationTime -Descending`) to identify any GPO modifications made during the exploitation window that could represent attacker-planted persistence via startup scripts or logon tasks.

Detection Guidance

Focus detection on Windows domain controllers and any Windows Server system running Netlogon. Key log sources: Windows Security Event Log, System Event Log, and network flow data.

Event IDs to monitor:

- 5805: Netlogon session setup failed; spike in these indicates brute-force or exploit attempts

- 4624 Type 3 (Network Logon) with unexpected source IPs, especially from external ranges

- 4625 with Netlogon as the authentication package and high failure frequency

- 4768/4769: Kerberos ticket requests from hosts not in the asset inventory

- 7045/4697: New service installation post-exploitation persistence indicator

Behavioral indicators:

- LSASS memory access by non-standard processes (potential post-exploitation credential dumping)

- Unexpected outbound connections from domain controllers to external IPs after Netlogon authentication events

- New scheduled tasks or services created on domain controllers within hours of Netlogon errors

Network indicators:

- Anomalous RPC (TCP 135) or SMB (TCP 445) traffic originating from external or untrusted network segments toward domain controllers

- Repeated connection attempts to Netlogon RPC endpoints from a single source IP

Refer to MITRE ATT&CK T1210 (Exploitation of Remote Services) and T1078.002 (Valid Accounts: Domain Accounts) detection guidance for additional hunting hypotheses. Per NIST AU-6 and CIS 8.2, these log sources must be actively collected and reviewed; gaps here are a control failure, not a detection miss.

Note: No confirmed IOCs (hashes, IPs, domains) were available from the source data. Behavioral detection is the primary mechanism until authoritative IOC feeds (CISA, Microsoft MSRC) publish indicators.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1078.002** — Domain Accounts

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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

Sources

Source	URL	Tier
	https://www.heise.de/en/news/Code-execution-possible-critical-vulne...	T3

Source	URL	Tier
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Microsoft Releases Emergency Patch for Exploited Critical Remote ...	https://arcticwolf.com/resources/blog/microsoft-releases-emergency-...	T3
Windows Server Update Service (WSUS) Under Active Exploitation ...	https://www.reddit.com/r/msp/comments/1oes768/windows_server_update...	T3
6 Actively Exploited CVEs – Patch ASAP! | Juan Pablo Castro	https://www.linkedin.com/posts/jpcastro_cybersecurity-patchtuesday-...	T3

Generated 2026-06-02 14:02 UTC by TJS Security Command Center