Technical Companion

Companion to: Domain Controller Patching Required: Netlogon RCE Under Active Exploitation Reference Bulletin Date: June 3, 2026 | For internal use and client technical response

Commands & Syntax Notice: Commands and code in this document are reproduced from cited sources as a reference only. Results may vary based on your environment, OS version, and tooling. Validate in a test environment before running in production.

IOC Notice: Indicators listed here reflect those reported by cited sources at time of publication and are not exhaustive. Threat actor infrastructure evolves — consult current threat intelligence feeds and your EDR/SIEM for the most complete picture. Absence of these indicators does not confirm a clean environment.

1. Patch Verification

Complete all steps below against every domain controller. Patch all DCs in the same maintenance window — a half-patched forest remains exploitable.

Step 1 — Identify All Domain Controllers

- Run the following from any domain-joined system with the Active Directory module: *(Source: Microsoft)*
  - `Import-Module ActiveDirectory`
  - `Get-ADDomainController -Filter * | Select-Object HostName, Site, IPv4Address, OperatingSystem, IsGlobalCatalog, IsReadOnly | Sort-Object Site, HostName | Export-Csv .\domain-controllers.csv -NoTypeInformation`
- Review the exported CSV to confirm all DCs — including branch site DCs, RODCs, and Server Core systems — are accounted for before patching.

Step 2 — Confirm Patch Status via Tenable

- Run the appropriate plugin for your Windows Server version against all DC IPs. See plugin reference table below. *(Source: Tenable)*
- Target DC subnets specifically — do not rely on a broad credentialed scan to surface these.
- A 'high' severity finding indicates the May 2026 cumulative update is absent.

Plugin ID	Plugin Name / KB Article	Direct Plugin URL
314355	KB5087539: Windows Server 2025	https://www.tenable.com/plugins/nessus/314355
314352	KB5087545: Windows Server 2022 / Azure Stack HCI 22H2	https://www.tenable.com/plugins/nessus/314352
314347	KB5087541: Windows Server 2022 23H2	https://www.tenable.com/plugins/nessus/314347
314346	KB5087538: Windows Server 2019	https://www.tenable.com/plugins/nessus/314346
314348	KB5087537: Windows Server 2016	https://www.tenable.com/plugins/nessus/314348
314354	KB5087470: Windows Server 2012	https://www.tenable.com/plugins/nessus/314354
314340	KB5087471: Windows Server 2012 R2	https://www.tenable.com/plugins/nessus/314340

Full plugin index: https://www.tenable.com/cve/CVE-2026-41089/plugins

Step 3 — Confirm Patch Installation via PowerShell

- On each DC, confirm the May 2026 KB is installed: *(Source: Microsoft)*
  - `Get-HotFix | Where-Object {$_.InstalledOn -gt (Get-Date).AddDays(-30)} | Sort-Object InstalledOn -Descending | Select-Object HotFixID, Description, InstalledOn | Format-Table -AutoSize`
  - Server 2025 — KB5087539
  - Server 2022 — KB5087545 (or KB5087541 for 23H2)
  - Server 2019 — KB5087538
  - Server 2016 — KB5087537
  - Server 2012 R2 — KB5087471
  - Server 2012 — KB5087470

Step 4 — Post-Patch Validation

- Verify AD replication is healthy after each DC is patched: *(Source: Microsoft)*
  - `repadmin /showrepl`
  - `dcdiag /test:replications`
- Confirm Netlogon service is running on each patched DC: *(Source: Microsoft)*
  - `Get-Service -ComputerName <DCname> -Name Netlogon | Select-Object Status, StartType`

2. Detection & Threat Hunting

Run these queries proactively across all DCs — not only in response to a confirmed incident.

Step 1 — Check for Netlogon Service Crashes

- Identify unexpected Netlogon service termination events: *(Source: CCB / Help Net Security)*
  - `Get-WinEvent -ComputerName <DCname> -FilterHashtable @{LogName='System'; Id=7034} | Where-Object {$_.Message -like '*Netlogon*'} | Select-Object TimeCreated, Message`

Step 2 — Check for New Privileged Account Creation

- Identify unexpected Domain Admin account creations: *(Source: Orca Security)*
  - `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4720} -MaxEvents 50 | Select-Object TimeCreated, Message | Format-List`
- Check for unexpected additions to privileged groups: *(Source: Orca Security)*
  - `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4728} -MaxEvents 50 | Where-Object {$_.Message -like '*Domain Admins*' -or $_.Message -like '*Enterprise Admins*'} | Select-Object TimeCreated, Message`

Step 3 — Check for NTDS.dit Access

- Requires object access auditing to be enabled. Monitor for unexpected access to the AD credential database: *(Source: Orca Security)*
  - `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4663} | Where-Object {$_.Message -like '*ntds.dit*'} | Select-Object TimeCreated, Message | Select-Object -First 20`

Step 4 — Network Detection

- In your SIEM or NDR, filter for the following: *(Source: CCB)*

- Inbound TCP 135 (RPC Endpoint Mapper) to DC IPs from hosts outside the DC subnet or known admin jump hosts
- High-volume short-duration connection attempts to DCs from a single external source
- Connections from DMZ, guest, or clinical device VLANs directly to domain controller IPs

3. IOC Reference Table

No specific threat-actor IPs, file hashes, or signatures have been publicly released at time of publication. Detection is behavior-based.

Type	Indicator	Detection Location / Method	Source
Behavior	**Netlogon service crash/restart**	Windows Event Log — System, Event ID 7034	*CCB / Help Net Security*
Behavior	**Anomalous RPC/Netlogon traffic from non-DC source**	Firewall/NDR — inbound TCP 135 + high ports to DC from unexpected hosts	*CCB / Help Net Security*
Behavior	**Auth failures after suspicious DC traffic**	Windows Security Log, Event IDs 4768/4771, 4625	*CCB*
Behavior	**New Domain Admin account creation**	Active Directory / SIEM — Event IDs 4720 + 4728	*Orca Security*
File	**NTDS.dit access or copy**	Monitor %SYSTEMROOT%\NTDS\ntds.dit access from unexpected processes (Event ID 4663)	*Orca Security*
Behavior	**Unexpected VSS shadow copy on DC**	Event ID 7036, vssadmin.exe spawning on a DC	*Orca Security*

4. Compensating Controls (If Immediate Patching Is Not Possible)

Apply ALL of the following for any DC that cannot be patched immediately. Document each exception with an owner and a firm remediation deadline.

Step 1 — Block Netlogon/RPC at the Network Layer

- Restrict inbound Netlogon/RPC to trusted DC sources only: *(Source: Orca Security / Help Net Security)*
  - Block TCP 135 (RPC Endpoint Mapper) inbound from non-DC source IPs
  - Block TCP dynamic high ports (49152–65535) inbound to the DC from non-DC hosts
  - If the DC is reachable from remote users, place it behind an application-layer gateway that inspects Netlogon-bound traffic

Step 2 — Apply 0patch for EOL Systems

- For Server 2008 R2, 2012, and 2012 R2, apply available micro-patches as an interim measure: *(Source: Microsoft / 0patch)*
  - `https://blog.0patch.com/`
- Plan decommission or in-place upgrade to a supported Server version in parallel.

Step 3 — Enable Enhanced Netlogon Logging

- Enable detailed Netlogon logging to detect exploitation attempts on unpatched DCs: *(Source: Microsoft)*
  - `nltest /dbflag:0x2080ffff`
  - Log output location: %windir%\debug\netlogon.log
  - Monitor for unexpected RPC call attempts or service errors in this log

Step 4 — Enforce MFA on Privileged Accounts

- Enforce MFA on all Domain Admins, Enterprise Admins, and Schema Admins immediately — limits blast radius if a DC is compromised. *(Source: Microsoft)*
  - MFA does not prevent CVE-2026-41089 exploitation but significantly constrains attacker lateral movement post-compromise

5. If Compromise Is Suspected

If exploitation indicators are confirmed on any DC, treat that controller as fully compromised and initiate your IR plan immediately.

Step 1 — Isolate the DC

- Remove the suspected DC from the network immediately. Do not attempt to remediate it in place. *(Source: Orca Security)*

Step 2 — Rotate the KRBTGT Account Password Twice

- Required to invalidate all outstanding Kerberos tickets across the domain: *(Source: Microsoft)*
  - `Set-ADAccountPassword -Identity KRBTGT -NewPassword (ConvertTo-SecureString -AsPlainText '<NewPassword>' -Force) -Reset`
- Wait at least the maximum Kerberos ticket lifetime (default 10 hours) between the two resets to ensure full propagation across all DCs.

Step 3 — Reset All Privileged Account Passwords

- Reset passwords for all Domain Admin, Enterprise Admin, and Schema Admin accounts. *(Source: Microsoft)*