Certighost (CVE-2026-54121): How Low-Privilege Users Impersonate Domain Controllers

Author: Synthex **Site:** denizhalil.com CVSS 8.8 HIGH **Date:** July 2026

INTRODUCTION

Active Directory Certificate Services (AD CS) serves as a foundational component in modern enterprise identity environments, facilitating public key infrastructure (PKI), machine authentication, VPN access, and smart card logins. However, misconfigurations and deep-seated flaws in how Enterprise Certificate Authorities (CAs) process incoming certificate requests or resolve directory objects can create severe privilege escalation vectors. The Certighost vulnerability (CVE-2026-54121) exposes a critical breakdown in this identity trust boundary, allowing an unprivileged or low-privileged Active Directory user to manipulate object resolution logic. By tricking an Enterprise CA into issuing a valid authentication certificate for a Domain Controller (DC) account, an attacker can seamlessly impersonate high-privilege administrative identities, leading directly to full domain compromise without ever possessing elevated credentials.

LEARNING OBJECTIVES

By reviewing this technical analysis, security professionals and system administrators will learn to:

- **Identify RPC Routing Fallbacks:** Learn how unvalidated RPC routing attributes (`cdc` and `rmd`) lead to remote identity spoofing.
- **Understand AD CS Architecture:** Gain deep architectural understanding of Active Directory Certificate Services (AD CS) and RPC query fallback behavior.
- **Trace Attack Chain Mechanics:** Follow the end-to-end attack chain enabling Domain Controller impersonation via Kerberos PKINIT and DCSync techniques.
- **Apply Hardening & Mitigations:** Deploy official security patches, configuration controls, and network-level mitigations to secure AD CS infrastructure.

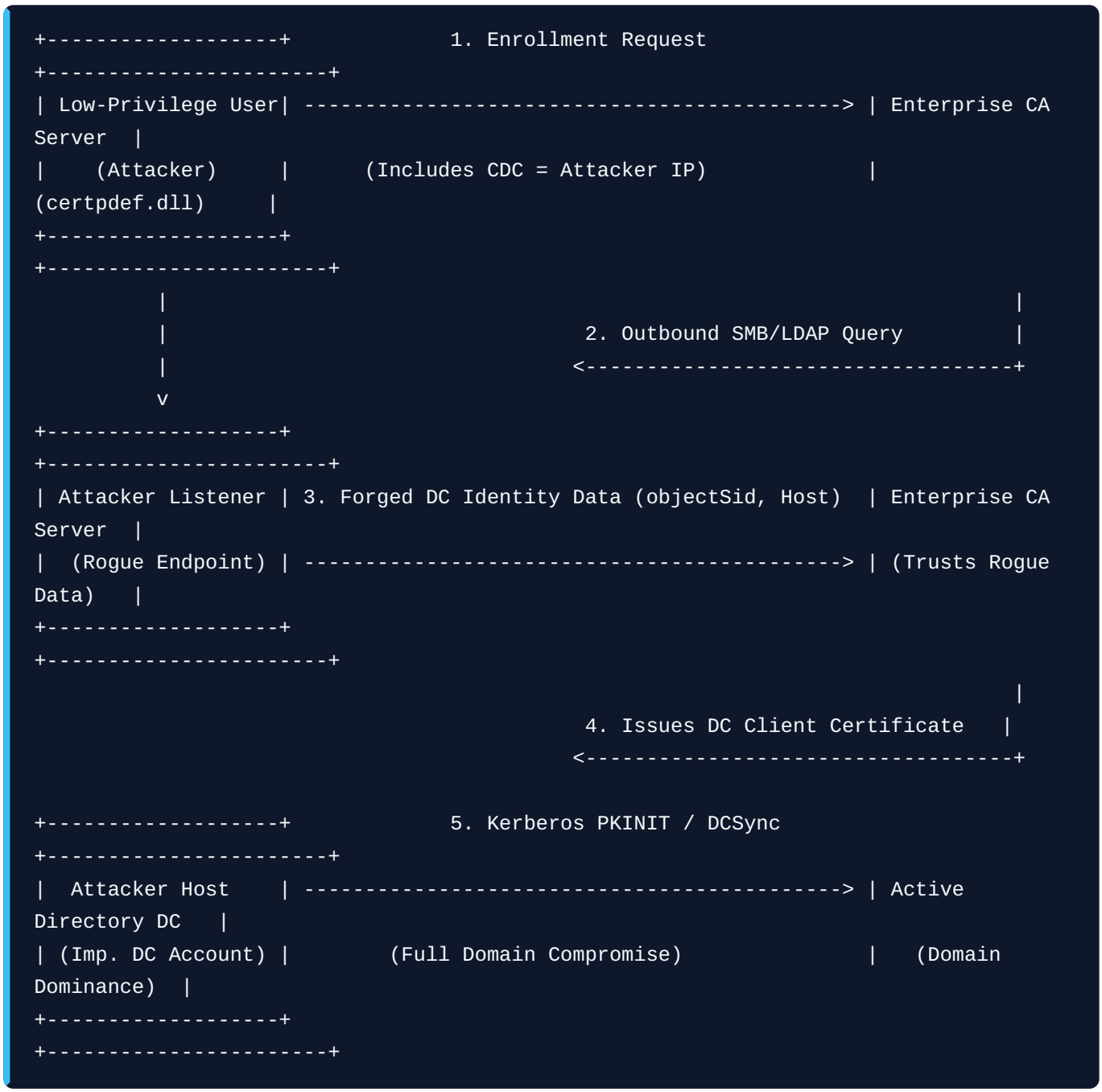
WHAT IS CERTIGHOST: LOW-PRIVILEGE ACTIVE DIRECTORY VULNERABILITY

Certighost (CVE-2026-54121) represents a fundamental breakdown in the authorization and identity verification logic of Active Directory Certificate Services (AD CS). In a secure Active Directory deployment, standard domain users are strictly prohibited from obtaining certificates that represent high-privileged assets, such as Domain Controllers or Enterprise Administrators. However, Certighost bypasses these traditional Access Control Lists (ACLs) and Role-Based Access Control (RBAC) boundaries

by exploiting an undocumented or loosely validated fallback path in how the Enterprise Certificate Authority (CA) resolves directory objects across remote procedure calls (RPC). The root cause of the vulnerability lies in the CA's "chase fallback" routine during the enrollment phase. When an incoming certificate request involves resolving remote machine identities, the CA relies on user-controlled routing parameters—specifically `cdc` (Client Domain Controller) and `rmd` (Remote Machine Descriptor). Because the CA fails to validate whether the target server specified in the `cdc` parameter is an authentic Domain Controller, an unprivileged user can force the Enterprise CA to establish outbound connections to an attacker-controlled endpoint. This allows the attacker to feed forged directory metadata directly into the CA's decision-making process.

As a result, the Enterprise CA becomes an unwitting proxy for privilege escalation. By trusting the forged identity data returned by the attacker’s rogue server, the CA issues a fully valid, digitally signed client authentication certificate bound to a legitimate Domain Controller machine account. The attacker can then leverage this certificate via Kerberos PKINIT to impersonate the Domain Controller, gain Directory Replication Service (DRS) rights, and dump domain credentials (such as the `krbtgt` hash) via a DCSync attack, resulting in complete Active Directory takeover.

- **Exploitation Prerequisites:** Requires only standard, low-privileged domain user credentials and network access to the Enterprise CA; no administrative rights or user interaction are needed.
- **Unvalidated RPC Chase Fallback:** The Enterprise CA blindly trusts user-supplied `cdc` parameters and opens outbound SMB/LDAP connections to untrusted IP addresses without verifying DC authenticity.
- **Identity Spoofing & Certificate Issuance:** The attacker's listener spoofs target DC parameters (`objectSid`, `dNSHostName`), prompting the CA to issue a legitimate X.509 certificate for the target DC account.
- **Full Domain Takeover:** The issued certificate enables Kerberos PKINIT authentication as a Domain Controller, granting the attacker DCSync privileges to extract all domain hashes.



TECHNICAL DETAIL: HOW THE VULNERABILITY WORKS

The technical architecture of the Certighost vulnerability centers on how Active Directory Certificate Services (AD CS) handles object resolution during certificate request processing. When a client submits a certificate enrollment request to an Enterprise CA, the underlying library (`certpdef.dll`) attempts to validate and map the requesting identity against Active Directory. If the CA cannot immediately locate the target object within its local domain cache, it initiates an RPC lookup fallback mechanism known as a "chase." Within this protocol context, the client is allowed to inject custom routing parameters—specifically `cdc` (Client Domain Controller) and `rmd` (Remote Machine Descriptor)—to instruct the CA on which domain controller should be queried to resolve the principal.

The core flaw stems from a complete absence of destination and boundary verification within `certpdef.dll`. When receiving a request containing a `cdc` parameter, the CA accepts the provided IP address or hostname without verifying whether the remote endpoint is a trusted, verified Domain Controller possessing the `SERVER_TRUST_ACCOUNT` flag. Consequently, the CA process executes an unauthenticated outbound SMB (TCP 445) and LDAP (TCP/UDP 389) connection directly to the address specified by the requester. When this destination points to an attacker-controlled listener, the attacker's rogue endpoint responds to the CA's directory queries with engineered LDAP metadata, returning the target Domain Controller's identity parameters (including its `objectSid`, `sAMAccountName`, and `dNSHostName`).

Because the Enterprise CA trusts the attributes returned by the controlled endpoint during the chase lookup, it binds the target DC's identity to the newly issued X.509 certificate. Once the signed certificate is issued, the post-exploitation phase transitions to Kerberos authentication. The attacker retrieves the certificate and uses PKINIT (Public Key Cryptography for Initial Authentication) to request a Kerberos Ticket Granting Ticket (TGT) on behalf of the Domain Controller's machine account (`DC01$`). Because Domain Controller accounts inherently possess Directory Replication Services (DRS) rights, the attacker can leverage the TGT to issue DCSync commands against the real DC, pulling sensitive account credentials—such as the `krbtgt` password hash—and securing complete domain dominance.

- **RPC Request Parameter Injection:** The attacker crafts an enrollment request containing custom `cdc` and `rmd` parameters pointing to an attacker-controlled IP address instead of a legitimate DC.
- **Unvalidated Outbound SMB/LDAP Connections:** `certpdef.dll` blindly initiates network queries to the specified `cdc` address without verifying if the target holds domain controller trust attributes.
- **Rogue Metadata Injection:** The attacker's listener intercepts the CA's LDAP queries and returns forged `objectSid` and `dNSHostName` values representing the target DC account.
- **PKINIT Credential Escalation & DCSync:** The resulting X.509 certificate allows the attacker to obtain a Kerberos TGT for the DC account and execute DCSync operations to extract all domain hashes.

```
[*] Certighost (CVE-2026-54121) Proof-of-Concept Execution Log
[*] Target Enterprise CA : CA01.corp.local (192.168.1.10)
[*] Target DC Account    : DC01$ (S-1-5-21-38291039-19283019-3910283-1001)
[*] Attacker Listener    : 192.168.1.150:389 (Rogue LDAP Endpoint)

[+] Step 1: Initiating certificate request with RPC chase parameters...
    |--> cdc parameter set to : 192.168.1.150
    |--> rmd parameter set to : DC01$

[+] Step 2: Enterprise CA initiated outbound query to 192.168.1.150:389
[+] Step 3: Rogue LDAP server responded with crafted directory metadata:
    |--> sAMAccountName : DC01$
    |--> dNSHostName    : DC01.corp.local
    |--> objectSid      : S-1-5-21-38291039-19283019-3910283-1001

[+] Step 4: CA validated response and signed X.509 client authentication certificate.
[+] Certificate successfully saved to: ./dc01_impersonated.pfx

[+] Step 5: Authenticating via Kerberos PKINIT as corp.local\DC01$...
[+] PKINIT TGT successfully acquired for DC01$!
[+] Executing DCSync (Replicating directory object: krbtgt)...

[SUCCESS] Domain Hash Extracted:
krbtgt:500:aad3b435b51404eeaad3b435b51404ee:e4a192b10293810293810293810293810293381:::
```

DEFENSE AND MITIGATION STRATEGIES

Securing Active Directory environments against Certighost requires a comprehensive, multi-layered defense model that addresses both the core vulnerability and common post-exploitation pathways. Because this attack vector relies on manipulating certificate enrollment target routing, relying on a single control is insufficient. Organizations must combine immediate patch deployment with proactive Active Directory hardening, tight network egress boundary controls, and continuous event auditing to effectively isolate Certificate Infrastructure and neutralize potential exploit attempts.

- **Apply Security Updates:** Deploy Microsoft's security patch for CVE-2026-54121 to update `certpdef.dll`. This enforces strict validation (`CRequestInstance::_ValidateChaseTargetIsDC`), ensuring any target supplied in `cdc` is a verified Domain Controller holding the `SERVER_TRUST_ACCOUNT` flag rather than an arbitrary IP address.
- **Restrict Machine Account Quota (MAQ):** Set the domain attribute `ms-DS-MachineAccountQuota` to `0`. Preventing standard non-administrative users from creating arbitrary machine accounts significantly reduces the attack surface for machine account exploitation.

- **Enforce Network Egress Controls:** Restrict outbound SMB (TCP 445) and LDAP (TCP/UDP 389) traffic from Certificate Authority (CA) servers, ensuring CAs can strictly communicate only with known, authorized Domain Controller IP ranges.
- **Monitor AD CS Event Logs:** Audit CA event logs specifically for Event IDs 4886 and 4887 to flag anomalous certificate requests containing custom routing parameters or unexpected machine account enrollments.

CONCLUSION

The Certighost vulnerability (CVE-2026-54121) serves as a stark reminder of how implicit trust in legacy protocol fallbacks can undermine the core security mechanisms of enterprise identity environments. By taking advantage of unvalidated RPC "chase" parameters, an unprivileged domain user can trick an Enterprise Certificate Authority into acting as a conduit for privilege escalation. This structural breakdown allows attackers to completely bypass standard access control lists and obtain high-privilege credentials without needing administrative access. From an architectural standpoint, the flaw highlights a critical failure in target validation within Active Directory Certificate Services (AD CS). When a Certificate Authority processes object resolution requests without verifying whether the target endpoint is an authentic, trusted Domain Controller, it exposes the entire domain hierarchy to identity spoofing. The ability to force the CA to establish outbound queries to arbitrary endpoints effectively allows attackers to manipulate the identity metadata bound to signed X.509 certificates. The post-exploitation consequences of this vulnerability are severe, as the issued certificates enable seamless authentication via Kerberos PKINIT. Once an attacker obtains a valid credential representing a Domain Controller machine account, they gain immediate access to Directory Replication Services (DRS). With these privileges, executing a DCSync attack to dump domain password hashes—including the critical `krbtgt` account—becomes a straightforward step, leading directly to full domain dominance.

Eliminating the threat posed by Certighost requires a proactive, multi-layered defensive posture. Organizations must prioritize applying vendor security patches to enforce strict target validation within `certpdef.dll`. In addition to patching, hardening Active Directory configurations—such as setting `ms-DS-MachineAccountQuota` to zero, enforcing outbound egress filtering on CA servers, and actively monitoring AD CS enrollment logs—is essential to ensuring long-term resilience against advanced AD CS attack vectors.