Security Risks and Attack Vectors

redfoxsec.com/blog/abusing-active-directory-certificate-services-a-comprehensive-guide

Kunal Kumar April 22, 2024

Abusing Active Directory Certificate Services: A Comprehensive Guide

- April 22, 2024
- Active Directory
- Kunal Kumar

Organizations operate in an ever-evolving digital environment that poses security threats. Although much attention has been focused on various components of Active Directory (AD), one often neglected area is Active Directory Certificate Services (AD CS), which offers encryption of file systems, digital signatures and user authentication features.

We will explore the security implications of AD CS and potential attack vectors that could be exploited. Additionally, we'll share tips and tactics for mitigating risks associated with misconfigured certificate service instances. This publication is tailored for security professionals, system administrators, and anyone responsible for protecting Active Directory environments.

Understanding Active Directory Certificate Services

1. AD CS is Microsoft's Public Key Infrastructure implementation, fully integrated into Active Directory. It issues digitally signed electronic documents (X.509 certificates) used for encryption, message signing, and authentication.
2. An identity can also be tied directly to its public/private key pair for proof of its existence in applications that utilize such keys as proof.
3. Certificate Authorities (CAs) are charged with issuing certificates, and AD CS serves as the infrastructure necessary to support this process.
4. Clients generate public-private key pairs, with their public key included in a Certificate Signing Request (CSR) message with other details like subject and template name; then send their CSR message to the Enterprise CA server, which verifies client eligibility before creating a certificate using template settings and signing it with the private key before returning it to the client.

The Role of Certificate Templates

Certificate templates play a crucial role in AD CS as they define the settings and policies that dictate the contents of a certificate issued by an Enterprise CA. These templates encompass various elements, including the certificate's validity period, its intended usage, the subject's specifications, and the allowed requesters.

The pKIExtendedKeyUsage attribute on a certificate template object contains an array of object identifiers (OIDs) that determine the certificate's usage. These Extended Key Usage (EKU) OIDs can enable authentication to Active Directory, such as the "Client Authentication" OID (1.3.6.1.5.5.7.3.2).

It's worth noting that certain EKUs, such as the 1.3.6.1.5.2.3.4 OID, need to be manually added to AD CS deployments but can be used for client authentication. Additionally, certificate templates have other settings that require further exploration, which we will cover in detail later in this guide. These settings, along with the template "Issuance Requirements," can serve as preventative controls against potential attacks.

Subject Alternative Names and Domain Escalation

Subject Alternative Names (SANs) are extensions that permit additional identities to be linked with certificates. While typically used to include multiple domain names in an HTTPS certificate, SANs can also be exploited as domain authentication mechanisms when used with certificates that permit domain authentication; an attacker could take advantage of misconfigurations by specifying any SAN they choose during certificate enrolment. If the CA creates and signs a certificate using the attacker's provided SAN, the attacker can assume the identity of any user in the domain.

This scenario can lead to domain escalation, where unprivileged users can elevate their privileges by requesting certificates with arbitrary SANs. Misconfigured certificate templates and insecure access control settings can enable attackers to abuse this vulnerability.

Active Directory Authentication with Certificates

Certificate-based authentication in Active Directory involves the use of certificates to authenticate users and machines. Traditionally, Kerberos has been the primary protocol for authentication, but Schannel, the security package backing SSL/TLS, is also utilized for domain authentication in certain scenarios.

LDAPS (LDAP over SSL/TLS) is an example of a protocol that supports client authentication via Schannel. With the appropriate configurations, certificates can be used to authenticate users and machines for various services, including LDAPS and other protocols that rely on Schannel

Rubeus, a popular tool for Kerberos-based authentication, can now request a Kerberos ticket-granting ticket (TGT) using a certificate enabled for domain authentication. This means that physical smart cards or the Windows Credential Store are no longer necessary for certificate-based Kerberos authentication. Additionally, some protocols, such as LDAPS, leverage Schannel for domain user authentication.

Account Persistence and Privilege Escalation

In addition to authentication, certificate services can also be leveraged for account persistence and privilege escalation. In environments with an Enterprise CA, users or machines can request a certificate for any eligible template.

By obtaining a certificate that allows authentication to Active Directory, an attacker can authenticate as that user or machine, even if their password is reset. This method of long-term credential theft bypasses the need to compromise the Local Security Authority Subsystem Service (LSASS) and can be performed from a non-elevated context.

Furthermore, certain misconfigurations in certificate templates and vulnerable access control settings can enable attackers to escalate their privileges within the domain. For example, misconfigured certificate templates (ESC1 and ESC2) can grant low-privileged users enrolment rights, bypassing manager approval and authorized signature requirements.

Overly permissive certificate template security descriptors can also grant certificate enrolment rights to unprivileged users. These misconfigurations, along with others detailed in the whitepaper, can result in domain escalation opportunities.

Vulnerable Certificate Template Access Control

Certificate templates are securable objects in Active Directory, meaning they have a security descriptor that defines the permissions granted to Active Directory principals. Misconfigurations in certificate template access control can allow unauthorized or nonprivileged principals to edit sensitive security settings within the template, potentially leading to unintended access, privilege escalation and potential security breaches. Such misconfigurations pose severe security risks.

To secure certificate templates, it is crucial to carefully configure the security descriptors and limit enrolment rights to authorized users. Implementing least privilege principles and regularly reviewing and updating access control settings can help protect against vulnerabilities in certificate template access control.

Certipy 4.0: Enhancing AD CS Security

- In recent years, Certipy, a powerful tool developed by Oliver Lyak, has emerged as a valuable asset for auditing and securing Active Directory Certificate Services.
- The latest version, Certipy 4.0, introduces new features and enhancements that further strengthen AD CS security.
- One notable addition is the integration of PKI support into the forked BloodHound GUI.
- This integration allows security professionals to visualize AD CS abuse primitives and gain insights into the relationships between certificate authorities, templates, and other AD objects.
- The forked BloodHound GUI provides a user-friendly interface with pre-built queries and the ability to copy queries to the clipboard for further analysis.
- Additionally, the Certipy tool itself has undergone improvements, reintroducing and enhancing features related to the find command.

New Authentication and Request Methods in Certipy

Certipy 4.0 introduces new authentication and request methods to enhance flexibility and usability. One significant addition is support for Schannel authentication, specifically LDAPS (LDAP over SSL/TLS). This feature allows users to authenticate via LDAP using certificates, providing an alternative to Kerberos-based authentication. By connecting to the domain controller and presenting the certificate during the StartTLS upgrade, Certipy enables seamless Schannel-based authentication.

Another noteworthy feature is Windows Integrated Authentication (SSPI) integration. This feature can be especially beneficial when the user credentials are unknown, such as when running code on a domain-joined machine. By leveraging Windows APIs to retrieve Kerberos tickets, Certipy can authenticate using the current user’s domain context. This integration streamlines authentication processes and ensures a smoother user experience.

Certipy 4.0 also introduces web enrolment capabilities, allowing users to request certificates through the web interface. This feature is particularly valuable in engagements where RPC-based certificate requests are not feasible. Additionally, the introduction of the double Subject Alternative Name (SAN) feature enables users to specify both DNS hostnames and User Principal Names (UPN) in certificate requests, providing greater flexibility and convenience.

Key Archival and Key Size Customization

To address specific requirements and configurations, Certipy 4.0 includes features related to key archival and key size customization. Users can now specify the desired key size using the -key-size parameter, ensuring compatibility with certificate templates that have different minimum key size requirements.

Furthermore, Certipy now supports certificate requests that require key archival. Key archival involves sending the private key during the request process to allow for storage and recovery by a designated Recovery Agent.

Certipy overcomes the challenges associated with key archival requests by employing CMC (Certificate Management over CMS) requests, encrypting the private key, and crafting the necessary structures to facilitate the process. With these enhancements, Certipy provides a comprehensive solution for handling various certificate request scenarios.

New Escalation Techniques: ESC9 and ESC10

- Building upon previous research, Certipy 4.0 introduces two new privilege escalation techniques for AD CS: ESC9 and ESC10.
- These techniques leverage vulnerabilities and misconfigurations to bypass security controls and elevate privileges within the domain.
- ESC9 exploits the “Validated write to DNS host name” permission on machine accounts.
- By duplicating the DNS hostname of a machine account, an attacker can gain unauthorized access and assume the identity of the target machine.
- This technique requires low-privileged access and the ability to perform Generic Write operations on a machine account.
- ESC10, on the other hand, takes advantage of Microsoft’s new security hardenings.
- By changing the values of specific registry keys to their old values, attackers can reintroduce vulnerabilities related to certificate mapping methods.
- These vulnerabilities can enable privilege escalation, allowing attackers to abuse certificate-based authentication in AD CS environments.

TL;DR

Active Directory Certificate Services (AD CS) is an integral component of modern IT infrastructure, offering crucial functions like encryption, authentication and digital signatures. However, misconfigurations and vulnerabilities can compromise AD CS’s security. This comprehensive guide has explored the security implications of AD CS and provided insights into various attack vectors and privilege escalation techniques.

To ensure the security of AD CS, it is crucial to follow best practices, regularly review and update access control settings, and implement strong security measures. Tools like Certipy can greatly assist in auditing and securing AD CS environments, offering features such as PKI integration, authentication methods, and request options.

Understanding potential threats and taking proactive security steps are effective ways for organizations to safeguard Active Directory environments and reduce any possible security breaches.

PreviousUnderstanding Buffer Overflow: Protecting Systems from Vulnerabilities
NextTenda N300 F3 Router Password Policy Bypass Vulnerability

Recent Blog