IDENTITY DAYS

netwrix

20 octobre 2026
PARIS

# ADCS

## Vulnérabilités ESC et stratégies de sécurisation

Hazem Taouai

**Hazem Taouai**

Lead Solution Engineer chez Netwrix, avec plus de 15 ans d’expérience en gestion des identités et des accès.

Dirige les démonstrations clients, les POC et les réponses aux appels d’offres à l’échelle mondiale.

# Agenda de la conférence

- Fondamentaux : qu'est-ce ADCS ?
- Les vulnérabilités ESC : vue d'ensemble
- Chaînes d'exploitation et impact
- Identification et audit des vulnérabilités
- Monitoring continu et détection d'anomalies
- Recommandations de sécurisation

# Active Directory Certificate Services

Infrastructure de gestion des certificats numériques intégrée à Active Directory. Émet, gère, renouvelle et révoque les certificats utilisés pour l'authentification, le chiffrement et la signature.

## Composants et rôles clés :

| | |
|---|---|
| **Root CA** | Racine de confiance - clé hors ligne |
| **Subordinate CA** | CA intermédiaire - émet les certificats |
| **Certificate Templates** | Modèles définissant les droits et les usages |
| **Enrollment Services** | Demande, validation et émission |
| **Certificate Manager** | Gère le cycle de vie et la révocation |
| **Online Responder** | Valide l'état des certificats |

*Fonctionnalités : Auto-enrollment • Renouvellement auto • Révocation rapide • Audit complet • Intégration native à AD*

# Flux d'émission de certificat

1

## 1. Demande

Un utilisateur ou une machine demande un certificat

2

## 2. Autorisation

Template et droits d'enregistrement vérifiés

3

## 3. Émission

CA signe et émet le certificat

4

## 4. Installation

Certificat stocké localement ou dans AD

5

## 5. Utilisation

Certificat utilisé pour auth, signature, chiffrement

# Vulnérabilités ESC : vue d'ensemble

**ESC (Escalation) : ensemble de mauvaises configurations d'ADCS permettant à un attaquant d'obtenir des certificats non autorisés et d'usurper l'identité d'administrateurs.**

*Documentées par Will Schroeder et Lee Christensen (SpecterOps) en 2021*

## Causes principales :

- Templates mal configurés permettant des demandes abusives
- Autorisations d'enregistrement trop permissives
- Enrollment Agent sans contrôle approprié
- Absence de validation des demandes

# Les 16 types de vulnérabilités ESC

**ESC1: Template SAN**
Le demandeur fournit le SAN

**ESC2: Any Purpose**
Template sans restriction d'usage

**ESC3: Agent Cert**
Demande au nom d'autrui

**ESC4: Template Perms**
Template modifiable (ACL)

**ESC5: PKI Objects**
ACL des objets PKI

**ESC6: CA SAN Global**
SAN autorisé par la CA

**ESC7: CA Control**
Droits ManageCA abusés

**ESC8: Web Relay**
Relais NTLM vers Web Enrollment

**ESC9: No SID Ext**
Template sans extension SID

**ESC10: Weak Mapping**
Mapping faible (registre)

**ESC11: RPC Relay**
Relais NTLM vers RPC

**ESC12: HSM Shell**
Accès shell sur la CA (HSM)

**ESC13: Policy Group**
Policy OID liée à un groupe

**ESC14: Explicit Mapping**
Mapping explicite altSecId

**ESC15: Legacy Policy**
Template V1 (EKUwu)

**ESC16: No Ext CA**
Ext. SID désactivée (CA)

# Chaîne d'exploitation typique

## 1. Reconnaissance

- Énumération ADCS
- Récupération templates
- Analyse AD

## 2. Sélection template

- Cibler un template
- Vérifier les droits
- Vérifier l'EKU Client Auth

## 3. Demande malveillante

- Usurper un admin
- Injecter le SAN
- Éviter les contrôles

## 4. Exploitation

- Utiliser comme jeton
- Pass-the-Cert vers le DC
- Accès Domain Admin

# Impact et risques

## Risques immédiats

- Usurpation d'identité d'un admin
- Contournement de MFA
- Accès administrateur persistant
- Mouvement latéral dans AD
- Modification des stratégies (GPO)

## Impacts métier

- Compromission de l'infrastructure
- Risque réglementaire
- Accès aux données sensibles
- Interruption de service
- Atteinte à la chaîne de confiance

# Identification des vulnérabilités : PingCastle

**PingCastle** : outil open source d'audit AD qui analyse les risques, y compris les mauvaises configurations d'ADCS et les vulnérabilités ESC.

## Capacités de PingCastle pour ADCS :

- Énumération complète de l'infrastructure ADCS
- Détection automatique des templates vulnérables (ESC1-4)
- Analyse des droits d'enregistrement sur les templates
- Identification des configurations dangereuses
- Score de risque dédié aux certificats
- Rapport détaillé avec recommandations

# Monitoring & Blocage : Threat Manager

**Threat Manager** : détecte ET bloque automatiquement les anomalies et comportements suspects dans Active Directory.

## DÉTECTION (Temps réel)

- Demandes anormales
- Utilisation malveillante
- Énumération ADCS
- Modifications de configuration
- Tentatives de Pass-the-Cert
- Corrélation d'anomalies

## BLOCAGE (< 1 minute)

- Révocation des certificats
- Isolement des comptes
- Blocage des connexions
- Désactivation des templates
- Alerte à l'équipe sécurité
- Arrêt immédiat

**Les attaques ESC ne sont PAS seulement détectées : elles sont STOPPÉES immédiatement (certificats révoqués, comptes isolés, attaquant bloqué).**

# Approche complète : audit + monitoring continu

**Diagnostic PingCastle** → **Remédiation & Hardening** → **Monitoring Threat Manager** → **Vérification continue**

1. **DIAGNOSTIC** : identifier les vulnérabilités existantes avec PingCastle
2. **REMÉDIATION :** corriger les configurations dangereuses et durcir ADCS
3. **MONITORING :** détecter les anomalies et les tentatives d'exploitation en temps réel
4. **VÉRIFICATION :** ré-auditer régulièrement, valider les corrections et détecter la dérive

# Recommandations de sécurisation

## Configuration des Templates

- Désactiver les enregistrements non supervisés
- Exiger l'approbation d'un gestionnaire de certificats pour Client Authentication
- Interdire la saisie du SAN par le demandeur
- Restreindre les droits d'enregistrement par groupe

## Durcissement de l'infrastructure

- Isoler les CA sur des serveurs dédiés (Tier 0)
- Segmenter le réseau autour de la PKI
- Chiffrer les communications CA-client (HTTPS + EPA)
- Mettre en place un audit complet des demandes

# Contrôles de détection à implémenter

## Logs et Événements

- Événement 4886 : demandes de certificats
- Événement 4887 : certificats approuvés et émis
- Centraliser les logs ADCS dans le SIEM
- Alertes sur modifications de templates (4899/4900)

## Analyse Comportementale

- Détection d'enregistrements inhabituels
- Utilisations impossibles de certificats
- Élévation utilisateur → administrateur
- Corrélation avec les événements AD suspects

# Comment PRÉVENIR les attaques ESC

| **AUDIT** *PingCastle* | **DÉTECTION** *Threat Manager* | **BLOCAGE** *Automatisé* |
|---|---|---|
| • Énumération ADCS | • Monitoring 24/7 | • Révocation des certificats |
| • Détection ESC1-4 | • Comportements suspects | • Isolement des comptes |
| • Analyse des permissions | • Corrélation d'anomalies | • Blocage des connexions |
| • Scoring des risques | • Alertes immédiates | • Arrêt en < 1 min |
| **Baseline** | **Visibilité** | **Prévention** |

**L'AUDIT identifie les vulnérabilités → la DÉTECTION repère les attaques → le BLOCAGE les arrête. Cycle continu : ré-audit trimestriel, monitoring 24/7 et réponse automatique en cas de tentative.**

netwrix

# Points clés à retenir

- ADCS est un composant critique dont les vulnérabilités peuvent compromettre tout le domaine
- Les vulnérabilités ESC exploitent des erreurs de configuration courantes
- L'audit initial et le monitoring continu sont complémentaires et indispensables
- La sécurité d'ADCS doit s'inscrire dans une stratégie globale de durcissement d'AD

# Ressources et références

- Will Schroeder & Lee Christensen : Certified Pre-Owned (2021)
- Documentation PingCastle : https://pingcastle.com
- Microsoft ADCS Best Practices & Hardening
- MITRE ATT&CK : Technique T1649 (Steal or Forge Authentication Certificates)
- Avis de sécurité : CVE-2022-26923 (Certifried), CVE-2024-49019 (ESC15)
- Communauté : Active Directory Security Community

IDENTITY DAYS
@IdentityDays
#identitydays2026