Exploiting AD CS: A quick look at ESC1 and ESC8

Active Directory Certificate Services offers important functionality, but it brings risks that organizations need to understand and mitigate.

Privilege escalation is the name of the game for annual penetration testers or attackers hoping to access sensitive information. Once attackers establish an initial foothold in an environment, often in the form of a compromised, low-level domain account, the next step is to escalate privileges via escalation (ESC) attacks. While privilege escalation comes in many, ever-changing flavors, attackers love to exploit Microsoft Active Directory™ Certificate Services (AD CS), so organizations should take steps to mitigate risks.

What is Active Directory Certificate Services?

AD CS is a Microsoft server role solution for public key infrastructure (PKI) that provides myriad services within an AD environment. AD CS can handle the public key cryptography, digital certificates, and digital signing needs of an entire organization, all with the benefit of having native integration with Active Directory. AD CS can provide certificate-based user authentication – which can be an extremely useful tool for managing an AD environment – but it can also be an extremely useful tool for compromising one.

Before diving into AD CS, detailing its inner workings can be helpful. Two important parts of AD CS to understand are certification authorities (CAs), commonly referred to as certificate authorities, and certificate templates. CAs are the servers that issue and manage certificates. Certificate templates are basically the bare-bones rule set used by AD CS to define the certificates that the CAs can distribute. Templates have a variety of attributes that control things such as who can request a certificate with said template; if approval is required to grant the request; if an existing certificate needs to sign off on the request; what kind of authentication is used to request the certificate; and who the certificate can be requested for. Certificate templates have many associated attributes. Exhibit 1 lists attributes that are important to ESC1 attacks.

Exhibit 1: Active Directory Certificate Services template attribute

Attribute	Meaning
msPKI-enrollment-flag	Whether CA manager approval is required
Authorized signatures required	How many authorized signatures are required to sign this certificate
PKI-extended-key-usage	What the certificate can be used for (for example, code signing and client authentication)
msPKI-certificate-name-flag	Whether the certificate be requested on behalf of another party
Enrollment permissions	Who can request a certificate with this template

Source: Crowe analysis, June 2023

Update notes

AD CS exploitation became mainstream around fall of 2021. SpecterOps published a critical article that brought to light glaring holes in security that were common to almost every production deployment of AD CS, which kicked off new efforts of AD CS exploitation. Since then, Microsoft has implemented changes that affect exploitation now and in the future. These changes, which SpecterOps detailed in a follow up, modified some escalation paths and completely cut others off. Let's take a look at how the updates affect the exploitation of ESC1.

An identity crisis?

With the KB5014754 update, the Microsoft Windows™ platform introduced strong and weak identity mappings. Weak, or implicit, identity mappings involve using information from the certificates' subject alternative name (SAN) extension, the domain name system, or user principal name field. Strong, or explicit, mappings, are the bread and butter of the update, and they bring changes to the original escalation paths. Explicit mappings use the altSecurityIdentities property to map a certificate to an identity, and three of these (X509IssuerSerialNumber, X509SKI, and X509SHA1PublicKey) are considered strong mappings. Microsoft categorizes these as strong mappings because they are based on identifiers that cannot be reused.

The new certificate extension, szOID_NTDS_CA_SECURITY_EXT will be used to facilitate strong identity mappings in most cases. This extension is intended to be used if there are no strong mappings present on a certificate, and it includes the security identifier (SID) of the requesting user. The idea here is the domain controller can check the SID of the authenticating user against this new security extension as a stand-in for a strong identity mapping. It is important to note that there are now three possible configurations for the StrongCertificateBindingEnforcement registry key that controls Kerberos authentication related to strong mappings, as Exhibit 2 shows.

Exhibit 2: Kerberos strong identity mapping settings

Setting	Description	Timeline
Disabled	Does not check for strong mappings	This option was removed on April 11, 2023.
Compatibility mode	Validates strong mappings or the szOID_NTDS_CA_SECURITY_EXT if they are present but will proceed with authentication if they are not	This option is the current default on all devices as of May 10, 2022.
Full enforcement	Requires a strong mapping or szOID_NTDS_CA_SECURITY_EXT to proceed with authentication	This option is set to become default on all devices Nov. 14, 2023, or later.

Source: Crowe analysis, June 2023

Exploitation

The first thing to understand about exploiting AD CS is that AD CS is not inherently vulnerable, with one little exception: human-made configuration decisions when creating templates. Let's break down ESC1 and ESC8, two common exploitations that result from such decisions.

ESC1

ESC1 is a quick and easy path from basic authentication to the domain administrator (domain admin). It is important to note that attackers need to have obtained initial authentication within the environment, but almost any user account will work for this attack. Once they have that initial foothold, attackers can make use of tools like Certify to enumerate vulnerable templates from the AD CS CA server. For ESC1 to work, all the following attributes must have specific values, as shown in Exhibit 3.

Exhibit 3: Required ESC1 template attributes

Attribute	Value
msPKI-enrollment-flag	None
Authorized signatures required	0
PKI-extended-key-usage	Client authentication or Smart card login or Any purpose or None (Subordinate CA)
msPKI-enrollment-flag	CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT
Enrollment permissions	Provides permissions to low-level domain users such as Everyone or Authenticated users

Source: Crowe analysis, June 2023

Following the KB5014754 update, ESC1 might require extra consideration. If the StrongCertificateBindingEnforcement registry key is set to compatibility mode (or disabled), all will proceed as expected. Once Microsoft pushes full enforcement in November 2023, attackers will have to supply the szOID_NTDS_CA_SECURITY_EXT value when making a certificate request. Many AD CS exploitation tools, such as Certify, have already been updated to include this functionality. Additionally, until full enforcement is pushed as a required configuration or optionally configured in the environment, attackers can exploit ESC1 without this consideration.

Once a vulnerable template with these attributes is identified, attackers are just a few steps from the domain admin. Using the low-level authentication that they have gained thus far, attackers can then use a tool such as Rubeus to request an authentication token from Kerberos (available to any user). The attackers then use Kerberos authentication to request a certificate using the vulnerable template and specify the request is on behalf of any domain admin they choose. Once attackers have that certificate, they then can simply request another Kerberos ticket-granting ticket (TGT) as the domain admin they requested the certificate for, and the domain admin is unlocked. Exhibit 4 demonstrates this process.

Exhibit 4: ESC1 in action

Source: Crowe analysis, June 2023

ESC8

Before discussing ESC8, a quick refresher on Windows New Technology LAN Manager (NTLM) relay attacks is useful. At a high level, NTLM attacks simply trick a machine or service into authenticating to the attackers. Attackers then redirect, or relay, that authentication to a destination they choose. Using this method, attackers can authenticate to machines or services without ever having to "own" the credentials they are using. There are many methods for tricking, otherwise known as NTLM coercion, the initial authentication and many methods for relaying that authentication to a new destination.

ESC8 uses the web enrollment interface feature of AD CS. AD CS web enrollment interfaces are optional features of AD CS, and they are commonly seen deployed alongside AD CS. These web enrollment endpoints are vulnerable to NTLM relay attacks because of the way they handle authentication. First, not all the web interfaces available from AD CS have HTTPS enabled, which is required to protect against NTLM relay attacks. In addition to being vulnerable to NTLM relay attacks, the CA must have at least one certificate template published that allows for client authentication and domain computer enrollment – again, a common template configuration. ESC8 can be used to target any domain macahine, including domain controller. All this combines to make AD CS web enrollment endpoints ideal for attackers that want to relay NTLM authentication and elevate their access.

What does an ESC8 attack targeting a domain controller look like in the wild? First, attackers can use a tool like Certify to enumerate the HTTP AD CS endpoints. Once an endpoint is identified, they can then use an NTLM coercion method such as the Windows Print Spooler bug or PetitPotam attacks to elicit NTLM authentication from a domain controller. That NTLM authentication is then relayed to the vulnerable AD CS web enrollment endpoint with a tool such as ntlmrelayx. The relay attack

requests a certificate for the domain controller. That certificate is then used to request a Kerberos TGT as the domain controller. The attackers now can authenticate as the domain controller anywhere in the domain, with access to whatever the domain controller machine account has access to. Exhibit 5 demonstrates this process.

Exhibit 5: ESC8 in action

Source: Crowe analysis, June 2023

Mitigation

AD CS is a vital component in enterprise-level environments for issuing and managing certificates. However, if it is not secured appropriately, it can become a significant target for threat actors to exploit through escalating privileges, executing code, and gaining access to sensitive data. Following are specific steps that organizations can take to mitigate these risks:

- Conduct a comprehensive risk assessment of the AD CS environment to identify vulnerabilities and potential risks
- Confirm that the AD CS infrastructure is appropriately configured and that best practices are in place
- Harden infrastructure by implementing security controls, such as:
  - Limiting access to servers only to authorized personnel and assigning least privilege access to those authorized
  - Configuring AD CS to require strong authentication and hardening configurations per updates from Microsoft
  - Implementing proper encryption protocols for all communications
- Implement continuous monitoring to detect any anomalous behavior
- Review and audit configurations; verify that all components are up to date with the latest security patches and updates
- Conduct periodic reviews of certificates and revoke any that are no longer needed or have been compromised

- Remove any unnecessary endpoints, especially AD CS web enrollment endpoints
- Implement a robust incident response plan in case of a security breach
- Restrict NTLM authentication in favor of Kerberos authentication wherever possible

By implementing these steps, organizations can mitigate the risks associated with threat actors exploiting AD CS through privilege escalation.

Mitigation tools

When it comes to mitigating attacks against AD CS, the most important step is to audit. It is important to get a view of the AD CS environment and take an inventory of the CAs and templates that are published by them. Once that information is in hand, the next step is to take a deeper look at the certificate templates to identify and remediate those that are vulnerable to exploitation. GhostPack's PSPKIAudit and Certify tools, as well others such as Certi and Certipy might be helpful in facilitating these processes. Additionally, BloodHound, a tool used for data visualization and Active Directory analysis, has been updated to ingest and visualize Certipy (similar to Certify) data. The combination of these two tools provides administrators with a powerful option to enumerate and audit their AD CS environments.

A proactive approach

Securing AD CS is a large undertaking, but by proactively implementing certain steps, organizations can mitigate the risks associated with threat actors exploiting AD CS through privilege escalation. One of the most powerful tools an organization can have is knowledge of their own infrastructure.

By conducting in-house audits or investing in third-party resources that can perform assessments for them, organizations can strengthen their cyber resilience and stay one step ahead of attackers that try to exploit their most critical infrastructure.