Active Directory Certificate Services: Risky Settings and How to Remediate Them

blog.netwrix.com/2021/08/24/active-directory-certificate-services-risky-settings-and-how-to-remediate-them

Joe Dibley

Active Directory Certificate Services has been around for a long time, but resources for learning it are not great. As a result, it often has misconfigurations that are an increasing vector for attacks. In fact, SpecterOps released a whitepaper detailing a number of misconfigurations and potential attacks and providing hardening advice. In this blog, I cover several of the settings that be misconfigured and how to spot them, offer several options for further hardening security, and explain how to use a free tool to check your environment.

Handpicked related content:
[Free Guide] Active Directory Security Best Practices

Background

When an authentication-based certificate is issued to an identity, the certificate can be used to authenticate as the identity set in the Subject Alternative Name (SAN); this is usually a UPN or DNS name. The certificate is then used in lieu of a password for initial authentication. The technical reference for this initial authentication is RFC4556 if you want to find out more detail.

Once an authenticated-based certificate has been issued, it can be used to authenticate as the subject until it is revoked or expired. This will circumvent incident response plans that rely on strategies like resetting the user's password to kick out an attacker; the attacker can have persistent access to the account unless the certificates are also revoked.

Handpicked related content:
Top 10 Most Common Types of Cyber Attacks

Risky Template Settings

Here are some of the certificate template settings that can lead to misconfigurations.

Authentication Based EKUs

First, look for Enhanced Key Usages (EKUs) that enable any kind of domain-level authentication. Here is a brief list:

- Any Purpose (2.5.29.37.0)
- SubCA (None)
- Client Authentication (1.3.6.1.5.5.7.3.2)
- PKINIT Client Authentication (1.3.6.1.5.2.3.4)
- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)

The easiest way to manually find all of your certificate templates that allow this is to open the Certificate Authority MMC Snap-in, connect to your Certificate Authority, look at the Certificate Template section and scan the Intended Purpose Column for any of these authentication EKUs. For example, the figure below shows that the Computer, Copy of Smartcard Logon and both Domain Controller templates contain at least one of the PKUs.

After you address the templates you find, be sure to keep in mind that there are ways to abuse normal certificates as well. For example, PoshADCS's Get-SmartCardCertificate function can modify a template, request certificates for it and then revert the changes to the template.

“Enrollee Supplies Subject” Flag

When the flag CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is present in the mspki-certificate-name-flag property, the enrollee of the certificate can supply their own alternative Subject Name in the certificate signing request. This means that any user who is allowed to enroll in a certificate with this setting can request a certificate as any user in the network, including a privileged user.

You can check this flag in the Certificate Template console; it’s under the Subject Name tab as the “Supply in the request” radio option:

Alternatively, you can use a PowerShell command like the following to get the templates from AD and check whether the flag is set in the certificate:

```
Get-ADobject -Filter { ObjectClass -eq "PKIcertificateTemplate" } -SearchBase (Get-
ADRootDSE).ConfigurationNamingContext -prop * | Select Name, mspki-certificate-name-flag, @{ Name =
"SupplyInRequest" ; Expression = { $_.'mspki-certificate-name-flag' -band 0x00000001 } }
```

Further Reducing Risk

In addition to correcting certificate misconfigurations, consider using the following options to control the issuing of certificates.

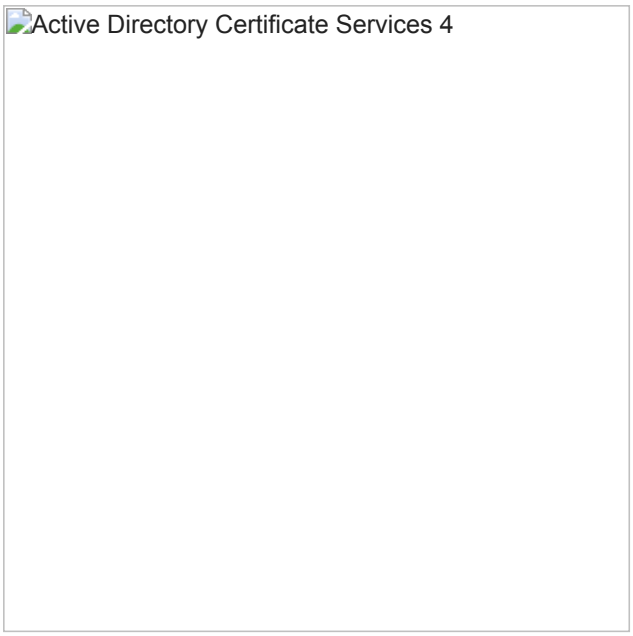
CA Certificate Manager Approval or Authorized Signatures

First and probably most important, look at the Issuance Requirements tab on each certificate to see if it requires approval from the Certificate Authority (CA) manager or one or more authorized

Enabling one or both of these settings can greatly reduce risk by requiring checks before certificates are issued. If you are unsure about requiring authorized signatures, at least require CA certificate manager approval; then every time a certificate is requested, it will go to the Certificate Authority for manual review before being issued.

Enrollment Permissions

Second, look at the enrollment permissions in each template, which can be found on the Security tab. Many misconfigurations are critical only when generic principals or large groups have these permissions. In particular, check for Authenticated Users, Domain Users and any large group of users who shouldn’t be able to request certificates; if you find them, consider revoking their Enroll or AutoEnroll permissions.



EDITF_ATTRIBUTESUBJECTALTNAME2 Registry Key

Last, check the EDITF_ATTRIBUTESUBJECALTNAME2 registry setting. This setting is one of the most interesting: If is enabled on the CA, then **any** authenticated-based certificate that is issued (including certificates where the subject is automatically built from Active Directory) can have user-defined values in the SAN.

To check this setting, you can run this command:

```
certutil –getreg policyEditFlags
```

If EDITF_ATTRIBUTESUBJECALTNAME2 is in the output list, you should remove it using this command:

```
certutil -config "CA CONNECTION STRING" -setreg policyEditFlags - EDITF_ATTRIBUTESUBJECTALTNAME2
```

Further guidance on this setting can be found here.

Checking for Risky Settings using PSPKIAudit

The PSPKIAudit tool can help you audit your PKI infrastructure. To use PSPKIAudit, simply download the tool from GitHub, import the module and run the Invoke-PKIAudit command. This will enumerate the Certificate Authority from Active Directory and then query it for some of the default options.

Below are a couple of screenshots showing the output of this tool, which reveals a misconfigured certificate and misconfigurations on the CA. If PSPKIAudit picks up any misconfigurations not covered in this post, check the SpecterOps paper for remediation advice.


Active Directory Certificate Services 5

Conclusion

I expect an increasing number of attacks on Active Directory Certificate Services. In fact, a PetitPotam with ADCS NTLM Relaying attack has already come out since the SpecterOps paper was published, and SpecterOps is releasing ForgeCert, the Golden Ticket of Certificates, at BlackHat 2021. Therefore, it's urgent to check for misconfigurations in your environment and remediate them promptly, and then to repeat the process on a regular basis.

For end-to-end protection, consider the Netwrix Active Directory security solution. It will help you:

- Proactively identify security gaps through an in-depth risk assessment.
- Minimize costly downtime and business disruptions.
- Promptly spot even advanced threats in time and respond quickly.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.