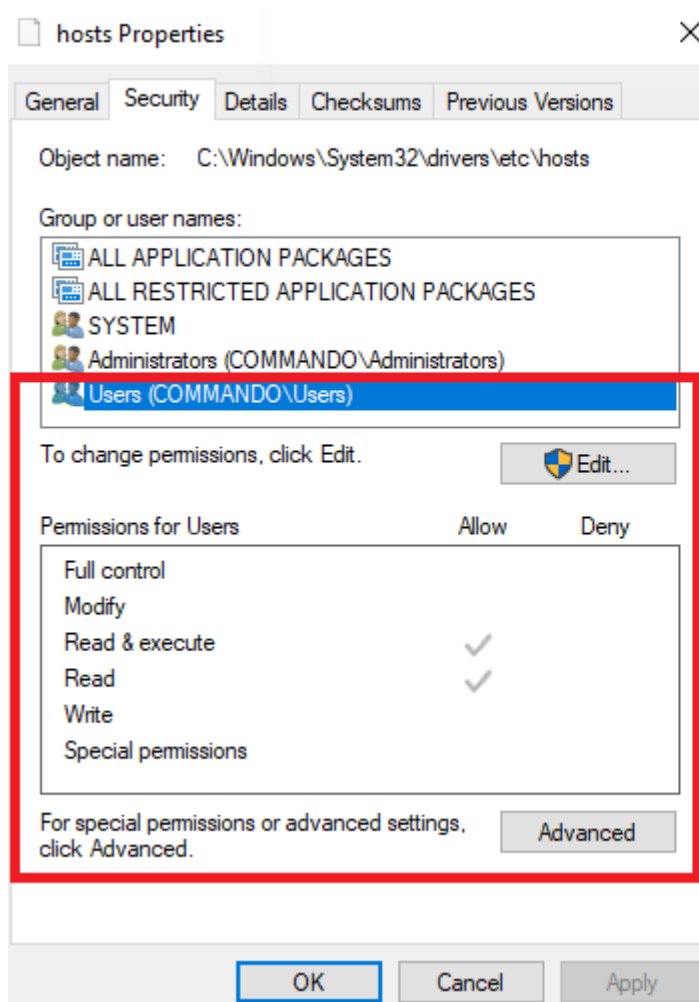
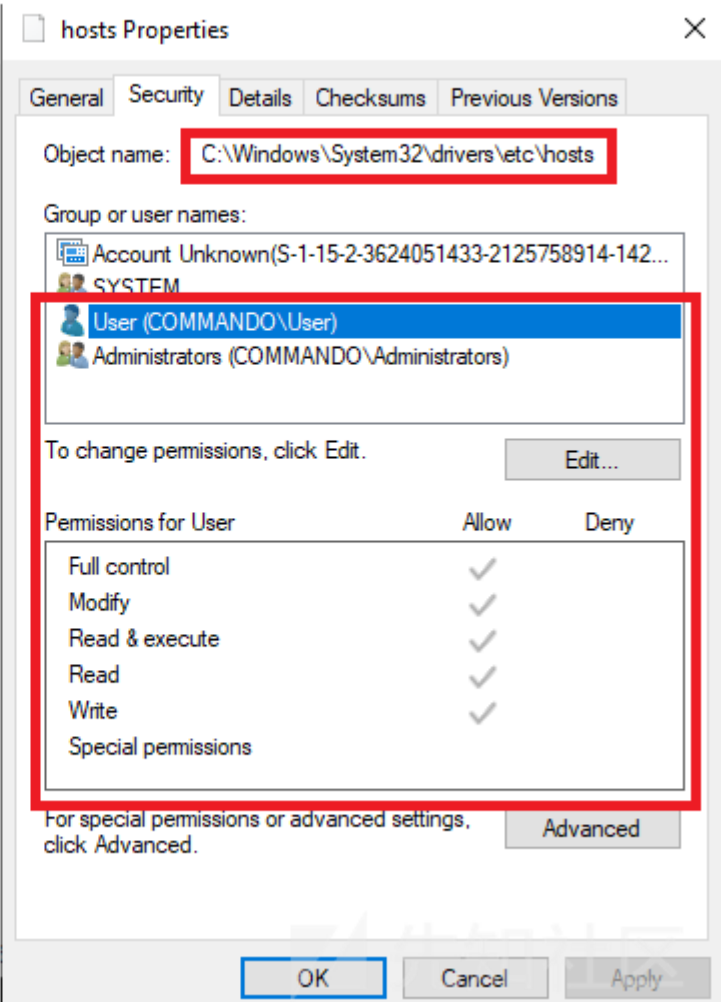


该漏洞允许低权限的用户通过覆写目标文件的权限来劫持属于NT AUTHORITY\SYSTEM的文件。成功利用就可以使低权限的用户获得对目标文件的完全控制权。

## BEFORE



## AFTER



所有的Windows APP都有一个settings.dat文件用来记录APP的注册表设置。该文件是一个可以在注册表中加载和修改的注册表文件。

如果用户启动一个Windows APP比如Microsoft Edge，就可以访问NT

AUTHORITY\SYSTEM的settings.dat文件，并以低权限用户访问该文件。问题是如何滥用该特权文件访问呢？

## 漏洞

首先看一下Microsoft Edge的settings.dat文件。

所有的Windows APPs用户配置文件都保存在当前用户的APPDATA文件夹：

C:\Users\<username>\AppData\Local\Packages\<Packagename>

PC > Local Disk (C:) > Users > nabeel > AppData > Local > Packages >					Search
Name	Date modified	Type	Size		
1527c705-839a-4832-9118-54d4Bd6a0c89_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
ActiveSync	1/28/2019 5:30 AM	File folder			
c5e2524a-ea46-4f67-841f-6a9465d9d515_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
E2A4F912-2574-4A75-9BB0-0D023378592B_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
InputApp_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
Microsoft.AAD.BrokerPlugin_cw5n1h2byewy	1/28/2019 5:30 AM	File folder			
Microsoft.AccountsControl_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
Microsoft.Advertising.Xaml_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.AsyncTextService_8wekyb3d8bbwe	1/28/2019 5:33 AM	File folder			
Microsoft.BingNews_8wekyb3d8bbwe	1/28/2019 5:55 AM	File folder			
Microsoft.BingWeather_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.BioEnrollment_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
Microsoft.CredDialogHost_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
Microsoft.DesktopAppInstaller_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.ECApp_8wekyb3d8bbwe	1/28/2019 5:33 AM	File folder			
Microsoft.GetHelp_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.Getstarted_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.LockApp_cw5n1h2byewy	1/28/2019 5:33 AM	File folder			
Microsoft.Messaging_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.Microsoft3DViewer_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.MicrosoftEdge_8wekyb3d8bbwe	1/28/2019 5:30 AM	File folder			
Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe	1/28/2019 5:33 AM	File folder			
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			
Microsoft.MSPaint_8wekyb3d8bbwe	1/28/2019 5:34 AM	File folder			

Windows 10有一些安装的默认APP

每个package都有一个settings.dat文件，是NT AUTHORITY\SYSTEM来写入配置变化的。

Windows App启动后，系统会使用OpLock操作来预防其他进程在APP运行时使用或访问该文件。

在本例中，启动Microsoft Edge后，settings.dat文件会以NT AUTHORITY\SYSTEM打开，如下图所示：

Process Name	PID	Operation	Path	Result	Detail
svchost.exe	4184	OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Read Control, Write DAC, Write Own...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	INVALID PARAM	
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: Owner, Group, DACL, SACL, Label, SACL Protected, DAC...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: SACL
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL, SACL, Label, SACL Protected, DACL Unprotected
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Re...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Sequential...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 73,728, EndOfFile: 71,680, NumberOfLinks: 2, DeletePe...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	BUFFER OVERFL	Information: DACL
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Data/List Directory, Write Data/Add File, Read...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 73,728, EndOfFile: 71,680, NumberOfLinks: 2, DeletePe...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	TotalAllocationUnits: 10,324,479, AvailableAllocationUnits: 5,850,797...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	BUFFER OVERFL	Information: DACL
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 0, Length: 512, Priority: Normal
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 4,096, Length: 512
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: N...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Attributes: AT, ReparseTag: 0x0
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Delete: True
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Attributes: A, ReparseTag: 0x0
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 8,192, EndOfFile: 8,192, NumberOfLinks: 3, DeletePenc...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 4/11/2018 3:34:39 PM, LastAccessTime: 1/25/2019 6...
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	0: :\$DATA
svchost.exe		OpenFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 4/11/2018 3:34:39 PM, LastAccessTime: 1/25/2019 6...

打开后，会看到执行一些基本的完整性检查：

#### 1. 检查文件权限

- 如果文件权限不准确，修正文件权限

#### 2. 读取文件内容

- 如果文件内容被破坏，就删除该文件
- 从其中复制设置模板文件来重置配置

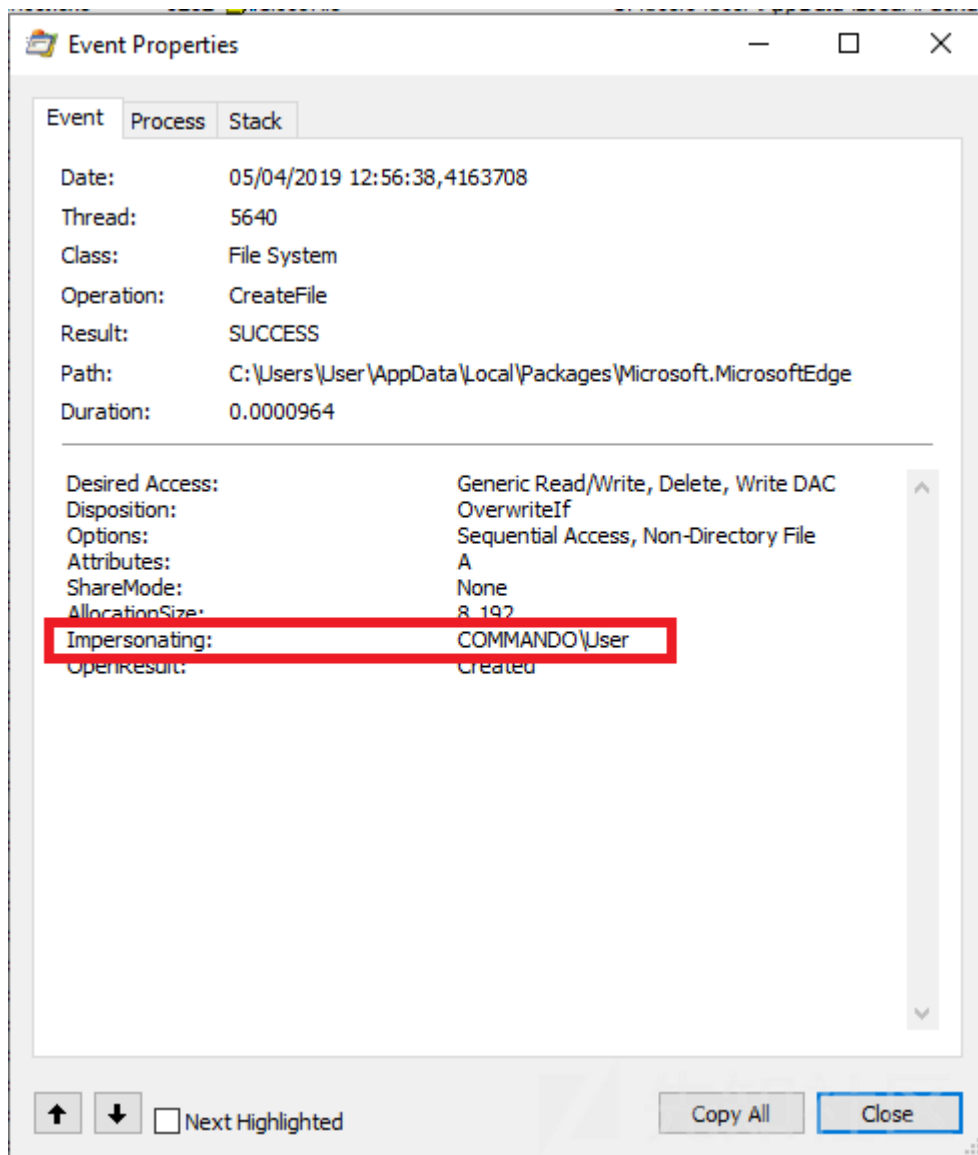
#### 3. 在新复制的文件上获取Exclusive Lock

#### 4. 启动Windows APP

该过程如下图所示：

Time	Process Name	PID	Operation	Path	Result	Detail	User
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Data/List Directory, Write Data/Add File, Read Control...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	SetBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 01/01/1601 01:59:58, LastAccess Time: 01/01/1601 01:59:59...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	FileSystemControl	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Allocation Size: 224, EndOfFile: 219, NumberOfLinks: 2, DeletePending: False...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStreamInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	TotalAllocationUnits: 39,163,903, AvailableAllocationUnits: 27,309,652, Sector...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	FlushBuffersFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	ReadFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 0, Length: 219, Priority: Normal	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 15/09/2018 09:31:35, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 15/09/2018 09:31:35, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Dire...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryAttributeTagFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Attributes: A, Reparse Tag: 0x0	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	SetDispositionInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Delete: True	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Windows\System32\settings.dat	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryAttributeTagFile	C:\Windows\System32\settings.dat	SUCCESS	Attributes: A, Reparse Tag: 0x0	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Windows\System32\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Windows\System32\settings.dat	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential Access...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Windows\System32\settings.dat	SUCCESS	Allocation Size: 8,192, EndOfFile: 8,192, NumberOfLinks: 2, DeletePending: Fa...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Windows\System32\settings.dat	SUCCESS	Creation Time: 15/09/2018 09:28:26, LastAccess Time: 15/09/2018 09:28:26...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStreamInformationFile	C:\Windows\System32\settings.dat	SUCCESS	0 : \$DATA	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Windows\System32\settings.dat	SUCCESS	Creation Time: 15/09/2018 09:28:26, LastAccess Time: 15/09/2018 09:28:26...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 05/04/2019 12:56:38, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: Overwri...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OpenFi...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryAttributeInformationVolume	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compr...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 05/04/2019 12:56:38, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryAttributeInformationFile	C:\Windows\System32\settings.dat	SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compr...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryRemoteProtocolInformation	C:\Windows\System32\settings.dat	INVALID PARAM...		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Windows\System32\settings.dat	SUCCESS	Information: Attribute	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 05/04/2019 12:56:38, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryNameInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Name: 'Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8we...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryRemoteProtocolInformation	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	INVALID PARAM...		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: Owner, Group, Attribute	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: Attribute	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	SetSecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Disposition: Attribute	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	SetBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	EndOfFile: 8,192	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	ReadFile	C:\Windows\System32\settings.dat	SUCCESS	Offset: 0, Length: 8,192, Priority: Normal	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	WriteFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 0, Length: 8,192, Priority: Normal	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	SetBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 01/01/1601 02:00:00, LastAccess Time: 01/01/1601 02:00:00...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryRemoteProtocolInformation	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	INVALID PARAM...		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Windows\System32\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse F...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryBasicInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 05/04/2019 12:56:38, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Creation Time: 05/04/2019 12:56:38, LastAccess Time: 05/04/2019 12:56:38...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Sequential Access...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	FileSystemControl	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QueryStandardInformationFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Allocation Size: 8,192, EndOfFile: 8,192, NumberOfLinks: 1, DeletePending: Fa...	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	QuerySecurityFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CloseFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS		NT AUTHORITY\SYSTEM
12:56...	svchost.exe	9232	CreateFile	C:\Users\User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SHARING VIOLAT...	Desired Access: Read Data/List Directory, Write Data/Add File, Read Control...	NT AUTHORITY\SYSTEM

绝大多数这些操作都是通过impersonating当前用户权限来执行的，这会防止滥用这些操作：



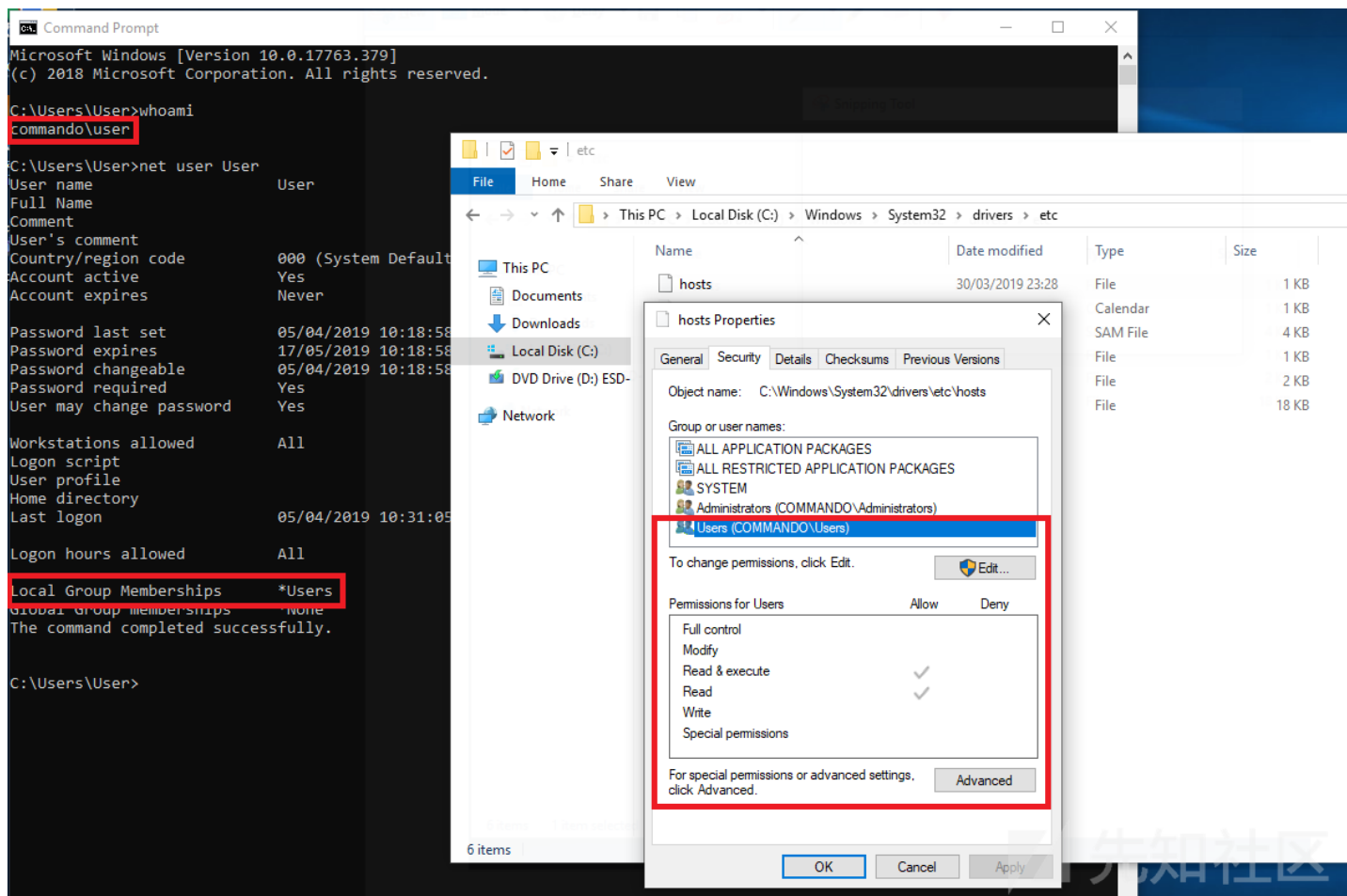
因此可以利用这一行为来对任意文件通过硬链接来设置文件权限。

## 漏洞利用

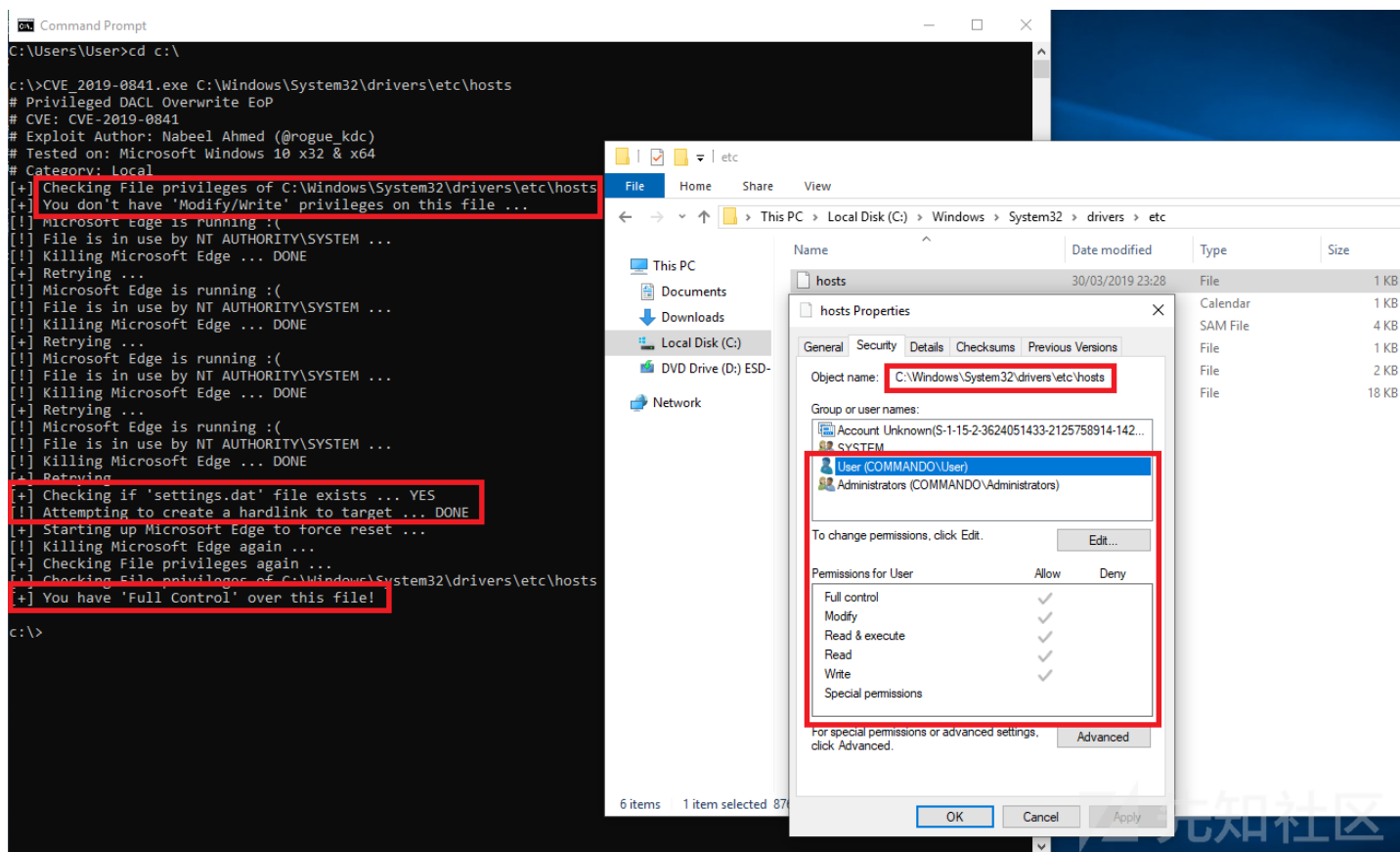
下面的漏洞利用过程是基于知识：设置硬链接的文件权限会改变原始文件的权限。

下面劫持位于C:\Windows\System32\drivers\etc\hosts的HOSTS文件。普通用户是没有该文件的修改访问权限的。





研究人员开发了漏洞利用可以自动创建硬链接并触发该漏洞，成功利用的结果如下图所示：



1. 漏洞利用首先检查目标文件是否存在，如果存在就检查其权限。研究人员使用Microsoft Edge来进行漏洞利用，它会杀掉Microsoft Edge的进程来获取settings.dat文件的访问权限。
2. Microsoft Edge被杀后，会检查setting.dat文件并删除该文件以创建到请求的目标文件的硬链接。
3. 硬链接创建后再次启动Microsoft Edge以触发漏洞。然后检查确认是否为当前用户设置完全控制权限。

研究人员同时指出一些漏洞利用所必须的条件：

- NT AUTHORITY\SYSTEM应该有对目标文件的完全控制权限；
- 低权限的用户或用户组应该有读写权限；
- 读和执行权限应该可以继承。

## PoC

PoC代码见：<https://github.com/roque-kdc/CVE-2019-0841>

Video PoC

[www.youtube.com/embed/vP468ZjJ3hU](https://www.youtube.com/embed/vP468ZjJ3hU)

POC视频证明了使用DLL和注入恶意代码来利用Chrome Update Service来进行权限提升，这也是完整利用该漏洞的过程。

<https://krbtgt.pw/dac1-permissions-overwrite-privilege-escalation-cve-2019-0841/>

点击收藏 | 1 关注 | 1

[上一篇：Hackerone 50m-ctf...](#) [下一篇：Hackerone 50m-ctf...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

---

[现在登录](#)

热门节点

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)