From: Lonny McMichael
Sent: Monday, September 09, 2002 6:32 AM
To: Brian Valentine; Jim Allchin
Subject: FW: Windows Media Player 9 Series

Any update on when WMP9 will be fixed to stop circumventing WFP?

Thanks, Lonny

---- Original Message ----
From: Jim Cavalaris
Sent: Monday, September 09, 2002 2:03 AM
To: Lonny McMichael
Subject: Windows Media Player 9 Series

fyi..

Windows Media Player 9 Series:
http://download.microsoft.com/download/winmediaplayer/WMPbeta/9/WXP/EN-US/mpsetupXP.exe

so on a whim, i decided to download and install the new media player 9 beta on one of my test machines, and set a few interesting breakpoints. (probably no surprises here):

```
kd> !process -1 0
PROCESS 8130fa68  SessionId: 1  Cid: 0460    Peb: 7ffdf000  ParentCid: 07d0
    DirBase: 0b145000  ObjectTable: e1076320  TableSize: 246.
    Image: setup_wm.exe

kd> !thread 81345da0
THREAD 81345da0  Cid 460.56c  Teb: 7ffdd000 Win32Thread: bc285c08
RUNNING on processor 0
IRP List:
    8153b5d0: (0006,0190) Flags: 00000000  Mdl: 00000000
Not impersonating
GetulongFromAddress: unable to read from 00000000
Owning Process 8130fa68
WaitTime (ticks)          163929
Context Switch Count      255                 LargeStack
UserTime                  0:00:00.0265
KernelTime                0:00:00.0203
Start Address kernel32!BaseThreadStartThunk (0x77e6d530)
Win32 Start Address msvcrt!_threadstartex (0x77c1917e)
Stack Init f9233000 Current f9232c4c Base f9233000 Limit f922f000 Call 0
Priority 8 BasePriority 8 PriorityDecrement 0
ChildEBP RetAddr  Args to Child
009cde74 0101b33e 000fdc78 009cde90 0000001f sfc!MySfcFileException (FPO: [3,0,0]) (CONV: stdcall)
009ce0a0 0101d34e 009ce0bc 009ce500 00000004 setup_wm!SetSFCFileException+0xc6 (FPO: [Non-Fpo]) (CONV: stdcall)
009ce4e0 01020ee2 009ce71c 00000000 009ce924 setup_wm!WMC_CopyFile+0x189 (FPO: [Non-Fpo]) (CONV: stdcall)
009ceb7c 010217a9 000b0db0 0026cfd8 00000001 setup_wm!CWMCInfParser::WMC_CopyFilesFromINFFile+0x3d2 (FPO: [Non-
Fpo]) (CONV: thiscall)
009cf1d8 0101534c 000b0db0 00000000 00000000 setup_wm!CWMCInfParser::InstallBasicINFFile+0x6a9 (FPO: [Non-Fpo])
(CONV: thiscall)
009cfe40 01019489 00000001 00000000 00000000 setup_wm!CWMCPackage::Install+0x40e (FPO: [Non-Fpo]) (CONV:
thiscall)
009cfe60 01019515 00000001 00000000 00000000 setup_wm!CWMCComponent::Install+0x16c (FPO: [Non-Fpo]) (CONV:
thiscall)
009cfe88 0100d9fd 00000000 00000001 00000000 setup_wm!CWMCComponentList::InstallPackageList+0x76 (FPO: [Non-
Fpo]) (CONV: thiscall)
009cff50 0100dc44 009cffb8 00000000 00263ec8 setup_wm!CWMInstaller::InstallFiles+0x169 (FPO: [0,42,3]) (CONV:
thiscall)
009cff80 0100dc8e 77c191ed 00263de0 00000000 setup_wm!CWMInstaller::StartInstallThread+0x1c1 (FPO: [EBP
0x009cffb8] [0,7,4]) (CONV: thiscall)
009cff84 77c191ed 00263de0 00000000 00000000 setup_wm!CWMInstaller::DoInstallThread+0xd (FPO: [1,0,0]) (CONV:
stdcall)
009cffb8 77e6d10c 00263e30 00000000 00000000 msvcrt!_threadstartex+0x6f (FPO: [Non-Fpo]) (CONV: stdcall)
009cffec 00000000 77c1917e 00263e30 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo]) (CONV: stdcall)
```

(btw, `sfc!MySfcFileException` is aka `sfc!SfcFileException`, is aka `sfc_os!SfcFileException`).

the corresponding server side RPC call is of course sfc_os!SfcSrv_FileException:

```
Breakpoint 2 hit
sfc_os!SfcSrv_FileException:
001b:76c5a548 55          push    ebp
kd> !process -1 0
PROCESS 815a1d88  SessionId: 0  Cid: 017c    Peb: 7ffdf000  ParentCid: 012c
    DirBase: 0f962000  ObjectTable: e13eb350  TableSize: 415.
    Image: winlogon.exe

kd> kb
ChildEBP RetAddr  Args to Child
00f5f908 77cf9d90 00e9a888 00157808 0000001f sfc_os!SfcSrv_FileException
00f5f928 77d1e374 76c5a548 00f5fae8 00000003 RPCRT4!Invoke+0x30
00f5fd04 77d1e5b1 00000000 00000000 00e9a9ac RPCRT4!NdrStubCall2+0x229
00f5fd20 77ccc687 00e9a9ac 00167d48 00e9a9ac RPCRT4!NdrServerCall2+0x17
00f5fd54 77cbd395 76c659d4 00e9a9ac 00f5fdf8 RPCRT4!DispatchToStubInCNoAvrf+0x17
00f5fda8 77cbe2a3 00000002 00000000 76c68090 RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0x112
00f5fdcc 77cb7ddd 00e9a9ac 00000000 76c68090 RPCRT4!RPC_INTERFACE::DispatchToStub+0xa1
00f5fe04 77cb9933 00e77a50 00e6f2e8 001577c0 RPCRT4!LRPC_SCALL::DealWithRequestMessage+0x2e1
00f5fe28 77cb9f48 00e6f320 00f5fe40 00e77a50 RPCRT4!LRPC_ADDRESS::DealWithLRPCRequest+0x16b
00f5ff8c 77cba188 77cbccd4 00e6f2e8 00000000 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x3e7
00f5ff90 77cbccd4 00e6f2e8 00000000 00000000 RPCRT4!RecvLotsaCallsWrapper+0x9
00f5ffb0 77cbad68 00085110 77e6d10c 00e6f3f0 RPCRT4!BaseCachedThreadRoutine+0x9c
00f5ffb8 77e6d10c 00e6f3f0 00000000 00000000 RPCRT4!ThreadStartRoutine+0x17
00f5ffec 00000000 77cbad51 00e6f3f0 00000000 kernel32!BaseThreadStart+0x34
```

this was called for each of the following files (appeared to be multiple times each):

```
009cde90  "E:\Program Files\Windows Media Player\npwmsdrm.dll"

009cde90  "E:\Program Files\Windows Media Player\npdrmv2.dll"

009cde90  "E:\WINDOWS\system32\drmclien.dll"

009cde90  "E:\WINDOWS\system32\drmstor.dll"

009cde90  "E:\WINDOWS\system32\drmv2clt.dll"

009cde90  "E:\WINDOWS\system32\blackbox.dll"

009cde90  "E:\WINDOWS\system32\msnetobj.dll"

009cde90  "E:\WINDOWS\system32\wmasf.dll"

009cde90  "E:\WINDOWS\system32\wmvcore.dll"

009cde90  "E:\WINDOWS\system32\wmnetmgr.dll"

009cde90  "E:\WINDOWS\system32\msdmo.dll"

009cde90  "E:\WINDOWS\system32\wmadmod.dll"

009cde90  "E:\WINDOWS\system32\wmsdmod.dll"

009cde90  "E:\WINDOWS\system32\wmvdmod.dll"

009cde90  "E:\WINDOWS\system32\mpg4dmod.dll"

009cde90  "E:\WINDOWS\system32\logagent.exe"

009cde90  "E:\WINDOWS\system32\laprxy.dll"

009cde90  "E:\WINDOWS\system32\wmadmoe.dll"

009cde90  "E:\WINDOWS\system32\qasf.dll"

009cde90  "E:\WINDOWS\system32\mswmdm.dll"

009cde90  "E:\WINDOWS\system32\msscp.dll"

009cde90  "E:\WINDOWS\system32\mspmsp.dll"

009cde90  "E:\WINDOWS\system32\wmdmps.dll"

009cde90  "E:\WINDOWS\system32\wmdmlog.dll"

009cde90  "E:\WINDOWS\system32\CEWMDM.dll"

009cde90  "E:\WINDOWS\system32\mspmspsv.dll"

009cde90  "E:\WINDOWS\system32\wmploc.dll"

009cde90  "E:\WINDOWS\system32\wmpshell.dll"

009cde90  "E:\WINDOWS\system32\asferror.dll"
```

```
009cde90  "E:\Program Files\Windows Media Player\wmplayer.exe"
009cde90  "E:\WINDOWS\INF\unregmp2.exe" (*)
009cde90  "E:\Program Files\Windows Media Player\setup_wm.exe"
```

all with the ExpectedChangeType flags parameter:

```
009cde84  0000001f
```

which is basically, all the defined `SFC_ACTION_*` flags, from `internal\base\inc\sfcapip.h`.

also ... is there any reason for `unregmp2.exe` (Microsoft Windows Media Player Setup Utility) to live in the *inf directory*? i noticed version 8 was already there on a clean install on .NET, even before i installed the version 9 beta?

-jim.