What is the significance of changing the registration for CLSIDs to point to a private copy of MSXML3?

devblogs.microsoft.com/oldnewthing/20160722-00

July 22, 2016

Raymond Chen

A customer reported that several of their applications stopped working after they installed a third-party program, let's call it Contoso Deluxe. They found that the Contoso Deluxe program, as part of its installation, rewrote some CLSID registrations. For example, `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F5078F37-C551-11D3-89B9-0000F81FE221}\InProcServer32` is normally `%SystemRoot%\System32\msxml3.dll`, but installing Contoso Deluxe changes it to `C:\Program Files\Contoso\Common\msxml3.dll`.

The customer wanted to understand the significance of this change.

The significance of this change is that the Contoso Deluxe program hijacked a bunch of objects that normally belong to the `MSXML3.DLL` that comes with the operating system, redirecting requests for those object to the private copy of `MSXML3.DLL` that comes with the Contoso Deluxe program.

I have two theories for why the Contoso Deluxe program does this. The more charitable theory is that the developers wanted to redistribute `MSXML3.DLL` and didn't know that there were specific instructions on how to do it correctly. Instead, they just packaged the DLL with their program and blasted the registry keys as part of installation.

If that's the case, then they should have followed the installation and redistribution instructions, so that the `MSXML3.DLL` file gets installed properly. Part of that proper installation is "If you see an existing copy of `MSXML3.DLL` that is newer than the one you are trying to install, then use the existing copy."

Another theory is that the developers found some sort of problem with newer versions of `MSXML3.DLL` and decided to solve the problem by locking their program to a specific version of `MSXML3.DLL` by packaging it with the program and directing all MSXML objects to their private copy of `MSXML3.DLL`.

If that were indeed their intention, then they tried to apply a global solution to a local problem. Because what they did was redirect all MSXML objects *for all applications in the system* to their private copy of `MSXML3.DLL`, even though they really wanted to redirect the object only for their program. The proper way to do this is to use an application manifest and registration-free COM to redirect the classes just for their program. (Of course, the real proper way to solve the problem is to figure out why their program doesn't work with newer versions of `MSXML3.DLL`.)

Note also that a private copy of `MSXML3.DLL` will not get serviced by Windows Update, which means that machines with that private copy will not receive security fixes to `MSXML3.DLL`. (More accurately, they will receive security fixes to `C:\Windows\system32\msxml3.dll`, which is useless because the system is using `C:\Program Files\Contoso\Common\msxml3.dll`.)

We advised the customer to engage with Contoso and work with them to fix the Contoso Deluxe program so that it neither breaks every program that uses `MSXML3.DLL`, nor prevents Windows Update from fixing security issues in `MSXML3.DLL`.

Raymond Chen

Follow