Deprecation of SHA-1 code signing

We are committed to continuing support of many of our customers' older operating systems. There are many scenarios, particularly in an industrial or medical environment where updating to the latest Windows version is impossible or prohibitively expensive. To this end, alongside our SHA-2 signature, till Reflect 7.3.5550, we have included a SHA-1 counter signature.

Due to the withdrawal of all SHA-1 timestamp services, we can no longer add a SHA-1 counter signature. This has two consequences for operating systems that haven't been updated to include SHA-2 support.

You will not be able to verify our binaries provenance or integrity. When launching Reflect, the publisher will be shown as "Unknown" in the Windows Vista and later UAC prompt. A user mode SHA-2 update is available for all Reflect supported platforms.

Where driver signature checks are enforced, drivers will not load without kernel SHA-2 support. Patches and updates for kernel SHA-2 support are only available for Windows 7 / Server 2008 R2.

Core Reflect features can only be implemented in kernel mode and therefore we are forced to block Reflect installs and updates in some instances, as detailed below.

Windows OS	Status
Windows 8, 10, Server 2016, 2019 and later	**SHA-2 is supported** by default, **no impact or action** required.
Windows XP, Server 2003 (32/64bit) and Vista 32bit / Win7 32bit	These OSs do not support SHA-2 by default, however due to lack of driver signature checks, **Reflect will continue to work** but you will receive an **unknown publisher warning** in the UAC prompt for Windows Vista and later. This can be resolved by applying a patch or updating to the latest release to gain user mode SHA-2 support.
Win 7 64bit / WIndows 2008 R2 Server 64 bit	Reflect updates and installs **beyond 7.3.5550 will continue to be supported** on this platform **if the OS has been patched to include SHA-2 support**.
Vista 64bit / WIndows 2008 Server 64 bit	**Reflect 7.3.5550 will be the last version available** for these platforms. This is due to a combination of enforced kernel driver signature checking without the availability of a kernel mode SHA-2 update from Microsoft.

Further References

https://redmondmag.com/articles/2019/02/19/windows-deadlines-sha-2.aspx

https://support.microsoft.com/en-gb/help/4472027/2019-sha-2-code-signing-support-requirement-for-windows-and-wsus