Under what conditions will the IUnknown::AddRef method return 0?

devblogs.microsoft.com/oldnewthing/20150312-00

March 12, 2015

Raymond Chen

A customer was debugging their application and discovered that for one of the objects they were using, the `IUnknown::AddRef` method returns 0. How is that possible? That would imply that the object's reference count was originally negative one?

The return value from `IUnknown::AddRef` is the object reference count by convention, but

> This value is intended to be used only for test purposes.

The return value is purely advisory and is not required to be accurate.

For example, if the object is a proxy, it will most likely return the reference count of the local proxy rather than the raw reference count of the original object. Conversely, if you have an object with outstanding proxies, the `IUnknown::AddRef` will count only one reference per proxy, even if the proxies themselves have reference counts greater than one.

The object the customer was using came from `MSHTML.DLL`, and it so happens that the implementation of `IUnknown::AddRef` used by that component always returns zero. It is technically within their rights to do so.

I don't know for sure, but I suspect this is done on purpose to avoid applications relying on the exact reference count. Applications are known to do dubious things, such as call `IUnknown:Release` in a loop until it says the reference count is zero. Making the objects return a value from `IUnknown::AddRef` that betrays no information about the object's true reference count may have been a defensive step to prevent applications from making any such dubious dependency.

If you install the debugging version of `MSHTML.DLL`, then the `IUnknown::AddRef` method will return the reference count. Which makes sense in its own way because the value is intended to be used only when debugging.

Raymond Chen

Follow