When can GetSecurityInfo API return ERROR_INSUFFICIENT_BUFFER?

devblogs.microsoft.com/oldnewthing/20170622-00

June 22, 2017

Raymond Chen

A customer reported that under stress testing, they found that when they call the `GetSecurityInfo` function to get the DACL of a job object, the call randomly returns `ERROR_INSUFFICIENT_BUFFER`. They can't find a pattern to the failure, and since the caller doesn't pass a buffer, it's not clear what buffer was insufficient. This happens even when the system is not under memory pressure, so it's not that the program itself was running out of memory.

What's going on is a race condition called out in the documentation:

> This function does not handle race conditions. If your thread calls this function at the approximate time that another thread changes the object's security descriptor, then this function could fail.

Basically, what happens is that internally, the function asks for the size of the security info, allocates the memory, and then asks for the buffer to be filled in. If the security information increases in size between the first and third steps, then the buffer passed in the third step is insufficient, and that's the error that is returned.

It's apparent from the fact that this race condition is called out that the function doesn't handle the TOCTTOU error and merely propagates the error back to you, making it up to you to retry (if that's what you want).

Personally, I think this is a flaw in the implementation.

Raymond Chen

Follow