Why does OpenProcess return access denied, even if I enable debug privilege?

devblogs.microsoft.com/oldnewthing/20151210-00

December 10, 2015

Raymond Chen

Many customers ask something like this:

> We want to get the creation time of a process, but our call to `OpenProcess` fails with `ERROR_ACCESS_DENIED`.
>
> ```
> struct KernelHandleDeleter
> {
>  void operator()(HANDLE *h)
>  {
>   if (h != nullptr) CloseHandle(h);
>  }
> };
>
> bool GetCreationTimeOfProcess(DWORD pid, FILETIME *creationTime)
> {
>  std::unique_ptr<HANDLE, KernelHandleDeleter>
>     process(OpenProcess(PROCESS_ALL_ACCESS, FALSE, pid));
>  if (!process) {
>   // GetLastError() returns ERROR_ACCESS_DENIED
>   return false;
>  }
>  FILETIME exitTime, kernelTime, userTime;
>  return GetProcessTimes(process, creationTime,
>                  &exitTime, &kernelTime, &userTime) != FALSE;
> }
> ```
>
> It works if the program is running as administrator, but not if the program is running as a standard user. We even enabled debug privilege, but that didn't help.

You don't have access because you don't have `PROCESS_ALL_ACCESS` permission on the process. `PROCESS_ALL_ACCESS` is a huge set of permissions, including `WRITE_DAC` (permission to change permissions), and if all you are doing is getting the process creation time, it's totally overkill. It's like getting power of attorney in order to be able to check their

cell phone bill. All you need in order to check someone's cell phone bill is to be listed as an *authorized person* on their account. You don't need permission to make like-and-death decisions on their behalf.

Getting the creation time for a process requires `PROCESS_QUERY_INFORMATION` or `PROCESS_QUERY_LIMITED_INFORMATION` access. So just ask for the minimum required to accomplish what you need. then you are more likely to get it.

```
bool GetCreationTimeOfProcess(DWORD pid, FILETIME *creationTime)
{
 std::unique_ptr<HANDLE, KernelHandleDeleter>
    process(OpenProcess(PROCESS_QUERY_LIMITED_INFORMATION, FALSE, pid));
 ...
}
```

Raymond Chen

Follow