How to electrify your own fence: ProcessStrictHandleCheckPolicy

devblogs.microsoft.com/oldnewthing/20161027-00

October 27, 2016

Raymond Chen

During process termination, if you try to enter a critical section that is owned by another thread that has already been terminated, the gates are now electrified, and the kernel simply terminates your process.

We saw that an invalid handle error and an object type mismatch error both mean that your critical section is corrupted.

And as noted in a comment on the last linked article, there is an option (enabled by default for Store apps) to electrify the fences and raise a exception if an application tries to use an invalid handle or an invalid type of handle (for example, trying to `SetEvent` on a semaphore). Classic Win32 applications can opt into this behavior by calling `SetProcessMitigationPolicy` and asking for the `ProcessStrictHandleCheckPolicy` to be turned on.

Raymond Chen

Follow