What is the window nesting limit?

devblogs.microsoft.com/oldnewthing/20031218-00

December 18, 2003

Raymond Chen

In the old days, Windows didn't bother enforcing a nesting limit because, well, if you want to nest windows 200 deep, that's your decision. Many window operations are recursive, but since everything happened on the application's stack, it was your own responsibility to make your stack big enough so it didn't overflow. But Windows NT moved the window manager off the application stack (first into a separate process, then into kernel mode). So now the OS needs to watch out for stack overflow attacks from people creating too many nested windows. The window nesting limit was set to 100 for the early days of Windows NT. For Windows XP, it dropped to 50 because increased stack usage in some internal functions caused us to overflow at around 75. Dropping to 50 created some breathing room.

Disclaimer: I was not personally involved in this issue. I'm just reporting what I was able to figure out from reading checkin logs.

Raymond Chen

Follow