It rather involved being on the other side of this airtight hatchway: Guessing window procedure magic cookies

devblogs.microsoft.com/oldnewthing/20190906-00

September 6, 2019

Raymond Chen

A security vulnerability report arrived that said that if you passed a carefully-malformed value to the `CallWindowProc` function, then it would call an unexpected function.

Recall that when you call `GetWindowLongPtr(GWLP_ WNDPROC)` and the window procedure's character set is different from the character set of th `GetWindowLongPtr`, then the window manager returns a magic cookie as the pretend window procedure. This magic cookie is meaningful only to the `CallWindowProc` function, and it indicates that the message parameters need to be changed from one character set to another before calling the *real* window procedure.

The finder wrote, "I haven't looked into it further to see any other possible security implications."

What are the security implications of letting people guess the magic cookies?

Nothing, really. Because you're already on the other side of the airtight hatchway.

Which made me kind of confused by that statement about "other possible security implications," since I couldn't even see the first one.

Remember, when looking at a potential security issue, you have to identify who the attacker is, who the victim is, and what the attacker has gained.

One possible attacker is "the process that passed an artificial magic cookie to the `Call-WindowProc` function." But all you're doing is attacking yourself. Even if the parameter happens to match an actual magic cookie, all you did was call a function in your own process. The `WPARAM` and `LPARAM` parameters might be transformed as part of the character set conversion, but really, what you found was a way to call a function in your own process in an extremely convoluted way.

Another attacker might be “an external entity which tricked a process into passing a crafted magic cookie to the `CallWindowProc` function.” But that means that the attacker found a way to trick a process into passing *a value of its choosing* to the `CallWindowProc` function. If an attacker has that much power over the process, then what’s it doing wasting its time with magic cookies? It can just trick the app into passing arbitrary function pointers to the `CallWindowProc` function! No need to limit yourself to functions that are callable via magic cookies; you can just call any function you like. In other words, the attacker gained nothing they didn’t already have.

Raymond Chen

Follow