It rather involved being on the other side of this airtight hatchway: If they can run code, then they can run code

devblogs.microsoft.com/oldnewthing/20070706-00

July 6, 2007

Raymond Chen

Some people can't get over the initial burst of adrenaline when they think they've found a security vulnerability and rush to file a report with Microsoft so they can get credit for it and add it to their "security vulnerability portfolio" to show that they are so wicked cool. Learning that what they found isn't a security vulnerability isn't going to stop them. "The `SPI_SNAPTODEFBUTTON` feature is a security hole. I can write a dialog box that keeps changing its default button, and the mouse will keep moving around to follow the new default button. Tada, I've hijacked your mouse!" — *Um, no, the "Snap to default button" feature doesn't work that way. It only snaps when the dialog first appears*. "Okay, well, then I can write a dialog box that hides and shows itself while it's changing its default button. That way, each time it shows, it yanks the mouse to the dialog's default button." — *That doesn't work either. It's on the first show that the mouse moves*. "Oh, okay, then I'll create and destroy the dialog in a tight loop. Each time the dialog box appears, it will yank the mouse. Aha, gotcha!" — *Well, sure, you can do that, but if your goal is to write an annoying program that yanks the mouse around, then this is an awfully inefficient way of doing it. Your annoying program should just call* `SetCursorPos`. You shouldn't be surprised that allowing people to run code lets them run code.

(Episode 1.)

Raymond Chen

Follow