It rather involved being on the other side of this airtight hatchway: Dubious escalation

devblogs.microsoft.com/oldnewthing/20100216-00

February 16, 2010

Raymond Chen

Consider this type of dubious security vulnerability:

> There is a buffer overflow bug in kernel driver X. To exploit it, call this function with these strange parameters. The exploit works only if you are logged on as administrator, because non-administrators will get `ERROR_ACCESS_DENIED`.

Yes, this is a bug, and yes it needs to be fixed, but it's not a security bug because of that *only if you are logged on as an administrator* clause.

It's another variation of the dubious elevation to administrator vulnerability. After all, if you're already an administrator, then why bother attacking kernel mode in this complicated way? Just use your administrator powers to do whatever you want to do directly. You're an administrator; you already pwn the machine. All you're doing now is flexing your muscles showing how cleverly you can take down a machine that's already yours.

Raymond Chen

Follow