It rather involved being on the other side of this airtight hatchway: Elevation to administrator

devblogs.microsoft.com/oldnewthing/20070920-00

September 20, 2007

Raymond Chen

Surprisingly, it is not a security vulnerability that administrators can add other users to the Administrators group. But that doesn't stop people from claiming that it is. For example, it's not uncommon for a vulnerability report to come in with the following steps:

1. (a) Install this rogue service/driver, or (b) copy this rogue program to your machine and change this registry key in `HKEY_LOCAL_MACHINE` to point to it, or (c) replace this file in the system directory with a rogue program.
2. Log on as an unprivileged user.
3. Perform magical operation X.
4. Boom! User is now an administrator!

Wow, this looks bad. An unprivileged user can elevate to administrator and... wait a second, what's that in step 1? To perform step 1, you need to have administrative privileges already. Only administrators can install services and drivers, only administrators can change registry keys in `HKEY_LOCAL_MACHINE`, and only administrators have write permission in the system directory. Therefore, this "vulnerability" basically says "If you can gain administrator privileges, then you can add anybody to the Administrators group." Well, sure, but you really chose the complicated way of doing it. Once you get administrator privileges, just do a `NET LOCALGROUP Administrators Fred /ADD` and you're done. After all, why write a service or a driver when a batch file does the trick just as easily? An alternative step 4 is "Boom! User is pwnzored!" Well, yeah, an administrator can install software that commandeers user accounts. This is hardly a surprise, is it?

In a sense, this is "security vulnerability by obscurity": By making your alleged exploit unnecessarily complicated, you can fool people into thinking that you're actually onto something.

Raymond Chen

Follow